

Vibration sensors are subject to a number of defeat techniques. These include;

- **Avoidance by using an entry method which does not require contact with the protected area;**
- **Muffling or dampening of the low frequency energy;**
- **Explosive penetration using limited force;**
- **Slow penetration to avoid meeting the threshold of pulse count and accumulator circuits;**
- **Spoofing and alarm stacking.**

Audio discriminator sensors can be defeated by:

- **Avoidance, muffling the noises associated with forced entry;**
- **Substitution of taped normal background noise to spoof the sensor;**
- **Bypass the sensor circuit while the system is disarmed;**
- **Mask the sensor microphone.**

#### **40\_3.2.3A Fence Vibration Sensor**



LSS401: Fence alarm system



LSS403: Shock sensors utilized to protect fences



**Figure LSS+4047** There are several different sensor technologies that are utilized to protect fences, including strain, vibration, and noise detection.

Higher frequency disturbances and greater amplitudes of events associated with sawing, cutting, climbing or lifting of the fence fabric generate mechanical vibrations or stress that can be differentiated from normal changes that occur from routine environmental activity. Fence vibration detectors are mounted directly on the fence webbing to detect these vibrations through electro-mechanical or piezoelectric transducers. The frequency characteristics for typical intrusion-type activity is filtered and processed and matched with known signatures.

Electro-mechanical sensors incorporate a signal processor that has a pulse accumulation circuit that recognizes momentary contact openings of electromechanical switches. Piezoelectric sensors have a signal processor that responds to the amplitude, duration, and frequency of the transmitted signal.

The Electromechanical Sensors use either **mechanical inertia switches** or **mercury switches** to detect fence vibration or stress. Mechanical-inertia switches consist of a vibration sensitive mass that rests on two or three electric contacts that create a closed-circuit. The mass is moveable and reacts to minute changes in the vibrations (frequencies) that are generated in the fence

during a penetration attempt. These vibrations disturb the mass, causing it to be moved or separated from one or more of the contact points, thereby momentarily opening the circuit and creating an alarm. In some sensor designs, the mass is intentionally constrained or restricted by an internal guide in order to ensure that only a significant vibration will cause movement, break the circuit and activate the alarm.

Mercury switches, as described elsewhere in this chapter, consist of a glass vial containing a small amount of mercury with a set of normally "open" electrical contacts that are located in close proximity, but not touching or immersed in the mercury. An impact or disturbance of the fence fabric causes the mercury to be displaced from its normal resting position. This will result in a momentary contact between the mercury (a conductor), and the electrical contacts.

A piezoelectric sensor is much like the old crystal microphone: it has the ability to convert the mechanical impact forces into an analog electrical output. Its output distinguishes it from the electro-mechanical sensor which can only generate an open or closed signal. The piezoelectric detector's output varies in proportion to the amplitude of the event. The signal is processed and filtered to match against known signatures.

For optimum performance, fence vibration sensors are mounted directly to the fence fabric. Each detector is connected in series along the fence with a common cable to form a single zone of protection. A zone length can have a recommended range of up to 300 feet. The vibration sensors are the most economical in their class and the easiest to install. They have a high probability of detecting intrusion and work well in protecting properly installed and maintained fence lines. Additional protection against tunneling and careful climbing can be achieved with the installation of in-ground vibration (seismic) sensors that are placed adjacent to the perimeter fence (in a controlled zone within the overall protected area).

Fine tuning of these systems is enhanced by adding information to the processor about current weather conditions to increase or decrease the detection sensitivity. A weather sensor station can be mounted on the fence line to feed information to a field processor, which then adjusts vibration alarm sensitivity, based upon weather data input.

Additional reliability can be obtained by placing the appropriate

volumetric motion detection devices (microwave, active infrared) along the perimeter of the fence. Which volumetric device to employ will depend upon the environment, terrain, and length of the fence line.

Vibration detectors are designed to sense many different variations and thus, can become confused and subject to false indication of an alarm status. In order to reduce the FAR, a pulse count accumulator may be added to the circuitry. This will require a threshold of pulses generated by individual trips in order to show a valid alarm status. A pulse is a measurable amount of activity (amplitude) based upon stress or vibration to the fence, caused by cutting or climbing.

Reliable operation of sensors is based upon their proper installation, and utilization on quality fencing material. Poor quality fencing with loose webbing can create "noise" from flexing, sagging or swaying that translates to false alarms and unreliable detection. Difficult weather conditions can add to the problem. Shrubbery, tree branches, and animals can also cause the fence to vibrate, thus triggering sensors. If fences are located in areas of high wind or numerous animal interactions, vibration sensors are not recommended. Remember, fence vibration detectors are designed for one specific function: to detect vibration. If they are located in areas with inherently high vibration, such as from railroad yards or tracks, construction sites, or heavy highway traffic, then they are not a suitable means of protection.

These detectors can be defeated by bridging the fence and thereby avoiding contact altogether. Use of overhanging trees and structures can assist in this regard, as can cars, trucks or other platforms. Deep tunneling is also a preferred method. Fence corners can be a particularly difficult problem because of the increased bracing of the fence posts and more solid foundations typically used at a corner or turn-point. Detectors will be less sensitive to input at these points because of the damping effect of the corner structures.

#### **40\_3.2.3A.1 Defeating Fence Vibration Sensors**





**Figure LSS+4056 A fence vibration sensor will trip from the use of hooks or a climber. Courtesy of DOE Office of Security and Safety Performance Assurance**

Electromechanical/vibration fence sensors can be defeated in a number of ways. These include:

- **Tunneling under the fence or barrier;**
- **Bridging, two-man or pole vaulting over the detection zone;**
- **Use a vehicle that is positioned next to the fence as a platform for jumping or bridging over the barrier;**
- **Injection of a dampening material into the sensor;**
- **Removal of the sensor from the fence, thereby preventing contact with the barrier;**
- **Alarm stacking.**

## VIBRATION FENCE SENSOR

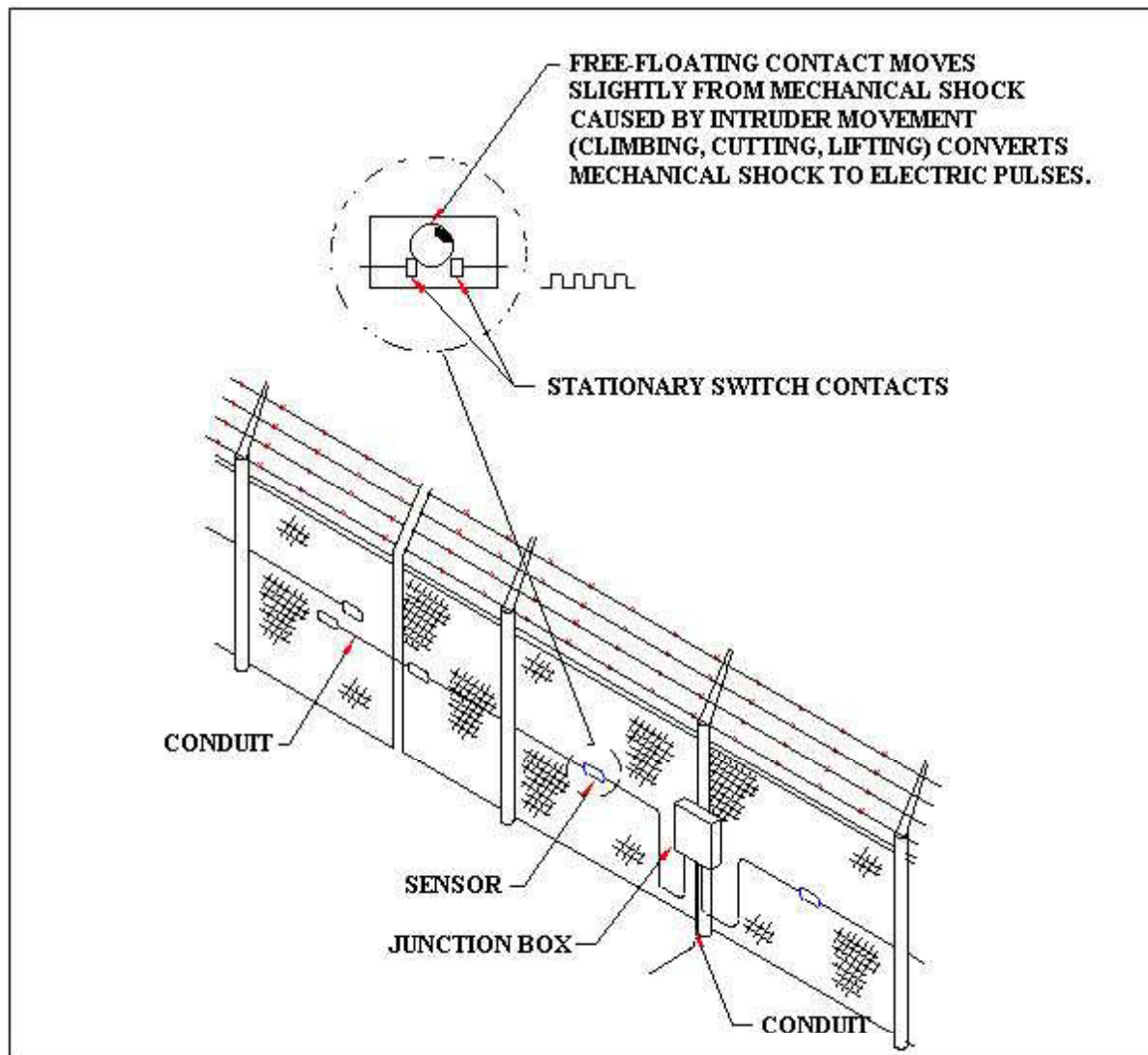


Figure LSS+4020 Vibration fence sensor

### 40\_3.2.3B Strain Sensitive Cable

Strain sensitive cables are line sensors that use electric energy as both a transmission and detection medium. They maintain constant sensitivity across the entire length of the circuit. Supervision against cutting, short circuit or removal of wire is maintained along the cable from the processor to an end-of-line resistor.

In operation, the cable is mounted on the fence. When it is subjected to mechanical vibrations that are caused by attempts to cut, climb or raise the fence fabric, electrical signals will be induced that are proportional (analog) to the exerted force, from which a signature analysis can be performed by the processor. The cable acts like a microphone.

There are two basic categories of strain sensitive cables: **coaxial** and **magnetic polymer**. The coaxial cable is a specially sensitized conductor in which the center conductor carries a permanent electrostatic charge.

The "coaxial" cable that is sensitive to strain related stresses conducts a permanent electric charge along its center conductor, which is then insulated and covered with a braided shield. The cable is designed for outside use, being coated with a UV resistant material to withstand direct sunlight. In operation, the cable is constantly electrically biased. When stresses occur based upon vibration, electrical signals are produced in proportion to the force exerted, and analyzed for specific signatures. The cable can act as a contact microphone to allow human analysis to evaluate a processor decision on alarm status. These detectors are extremely sensitive to EMI (electro-magnetic interference) caused by power substations and to radio frequency interference (RFI). Care should thus be exercised in the location of such sensors.

The magnetic polymer utilizes two semicircular magnetic polymer conductors that are separated by an air gap containing two noninsulated wires, resembling the design of a capacitor. Strain sensitive sensors function as poles of a linear magnet; two semicircular magnetic polymer conductors are paired and separated by an air gap. Two insulated wires run between the polymers. Parallel to these wires are two noninsulated wires free to move in the air gap between the magnetic field created by the polymer conductors.

Vibration and stress can cause the noninsulated wires (active conductors) to move within the air gap, generating minute electric signals to the signal processor. Smart processors are available that "learn" from normal fence fluctuations and revise the data, thus minimizing false alarms and enhancing the performance of the system.

The "magnetic polymers" multiple conductors form a symmetrical and balanced pair configuration that makes this type of sensor

virtually impervious to both EMI and RFI. Its low impedance creates higher signal-to-noise ratios that can offer more finite signal processing. The sensor also functions as a transducer microphone that can provide a "listening" function for human override and analysis.

Cables should be installed using ties halfway between the bottom and the top of the fence. Also, stainless steel wire ties, as opposed to plastic ties, should be utilized to prevent silent removal by burning or ultraviolet decay. Sensor zone lengths can be extended to 1,000 feet, with the requirement of a quality fence and stable installation of both the sensors and fence line. Supplemental protection should be implemented. Volumetric motion detection devices, video motion detection, and electric field detectors can add reliability and redundancy to a system.

Nuisance and false alarms can be caused by severe weather conditions and animals. This problem can be minimized with proper calibration and installation, and the use of a listening device to analyze signals. Countermeasures for this type of sensor are the same as for other fence line protection systems discussed above.

#### **40\_3.2.3B.1 Defeat of Strain Sensitive Cables**

Strain sensitive cable sensors can be defeated by a variety of methods, including:

- Tunneling or trenching under the sensor. An alarm will not be initiated unless there is contact with the fence;
- Pole or two-man vaulting or bridging;  
Avoidance of protected area;
- Bridging of protected area with board, ladder, or other structure;
- Bypass the sensor circuit while the system is disarmed;
- Creating small holes in the cable jacket (with pins or other sharp object) to allow water or moisture to enter and desensitize the cable. This is a long-term method of defeat and will require several days or months to accomplish;
- Remove the cable from the fence by gently severing or melting the wire ties, and then lowering the cable to the ground. This technique is accomplished over a period of time and takes advantage of poor fence inspections;
- Alarm stacking.

LSS+ Electronic Infobase Edition Version 5.0

2452 22/09/2007 11:42:38 AM  
(c) 1999-2004 Marc Weber Tobias

### STRAIN - SENSITIVE CABLE (COAXIAL)

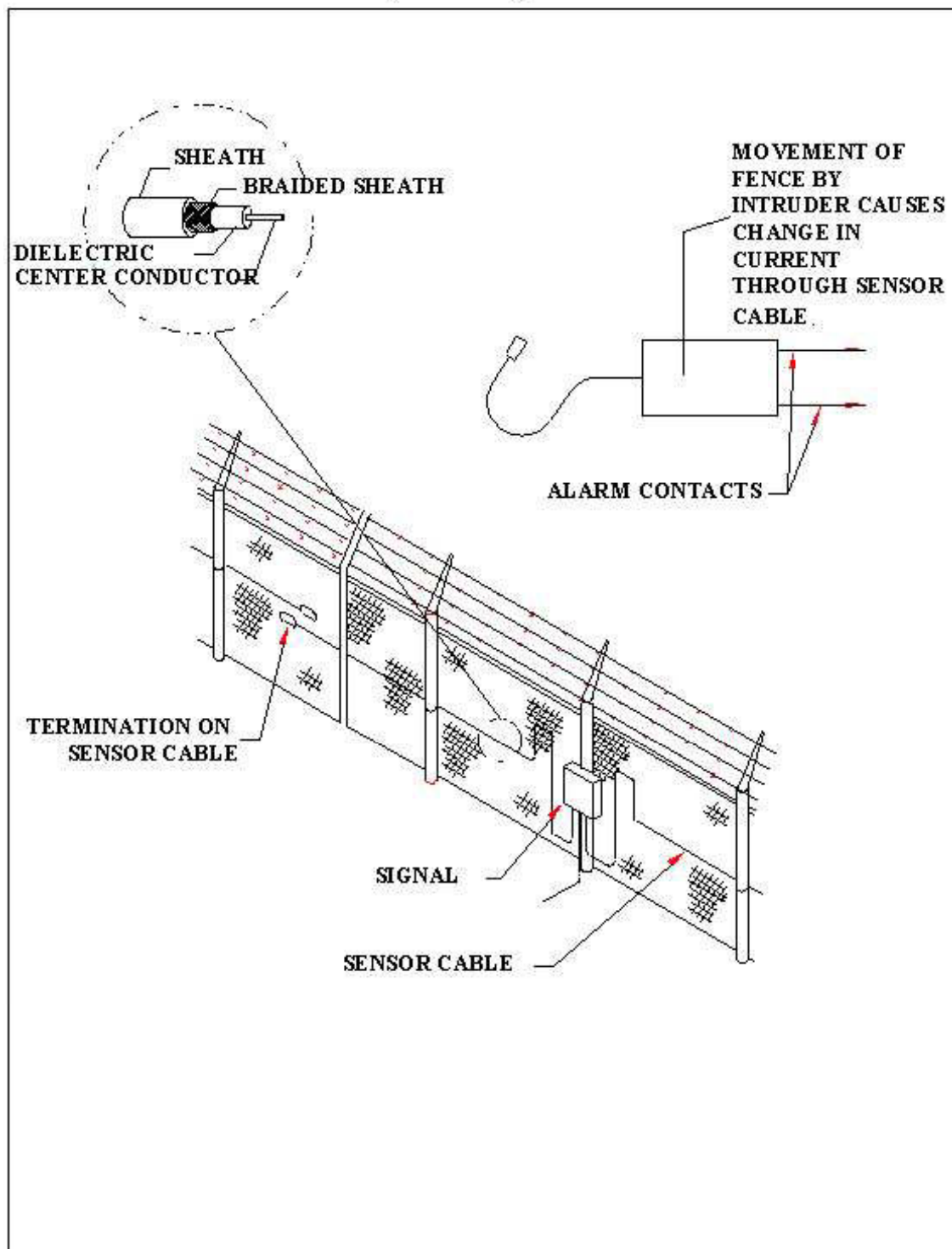




Figure LSS+4023 Strain-sensitive cable (coaxial)

**STRAIN SENSITIVE CABLE (MAGNETIC)**

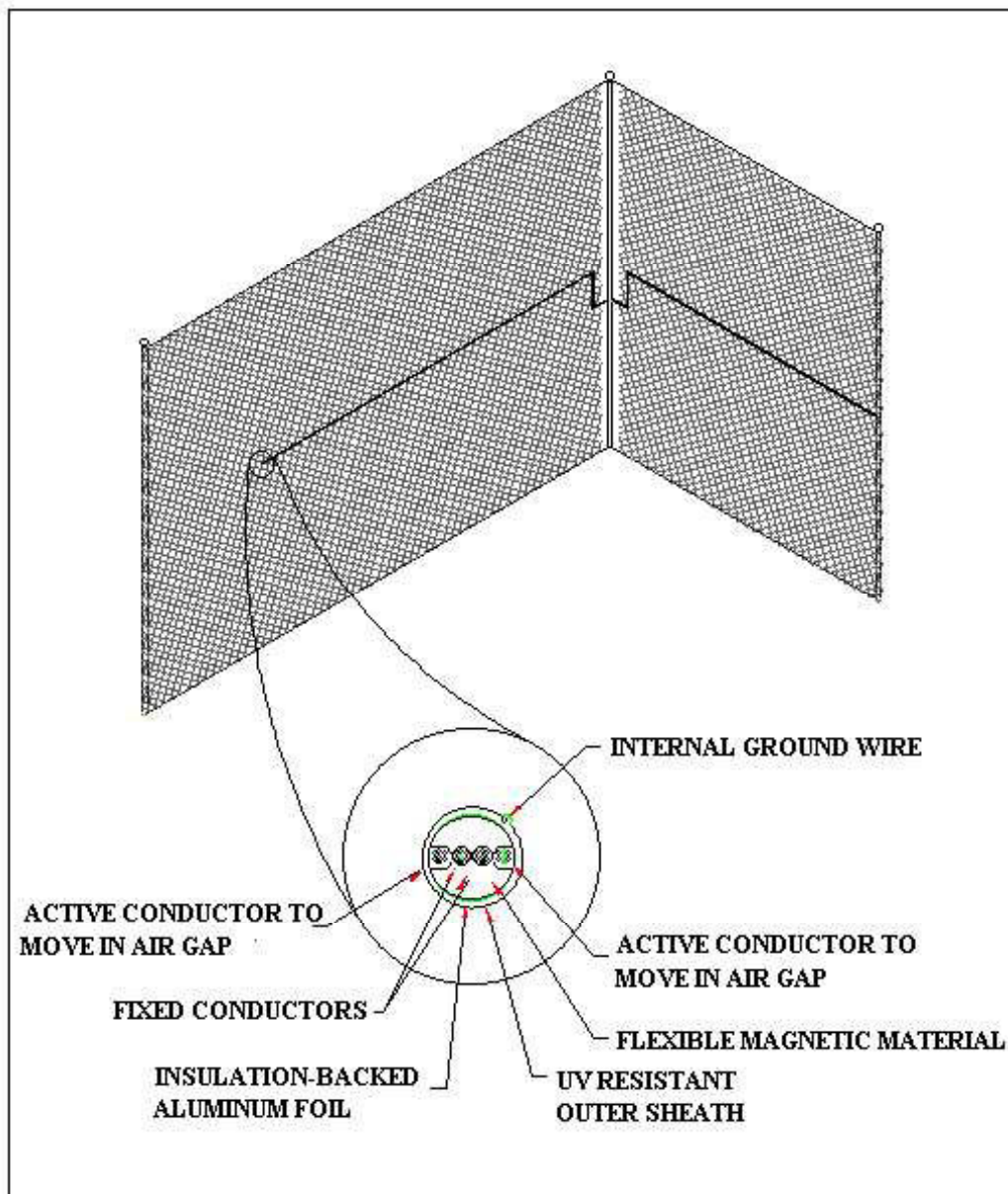


Figure LSS+4024 Strain cable (magnetic)



## STRAIN - SENSITIVE CABLE (APPLICATIONS)

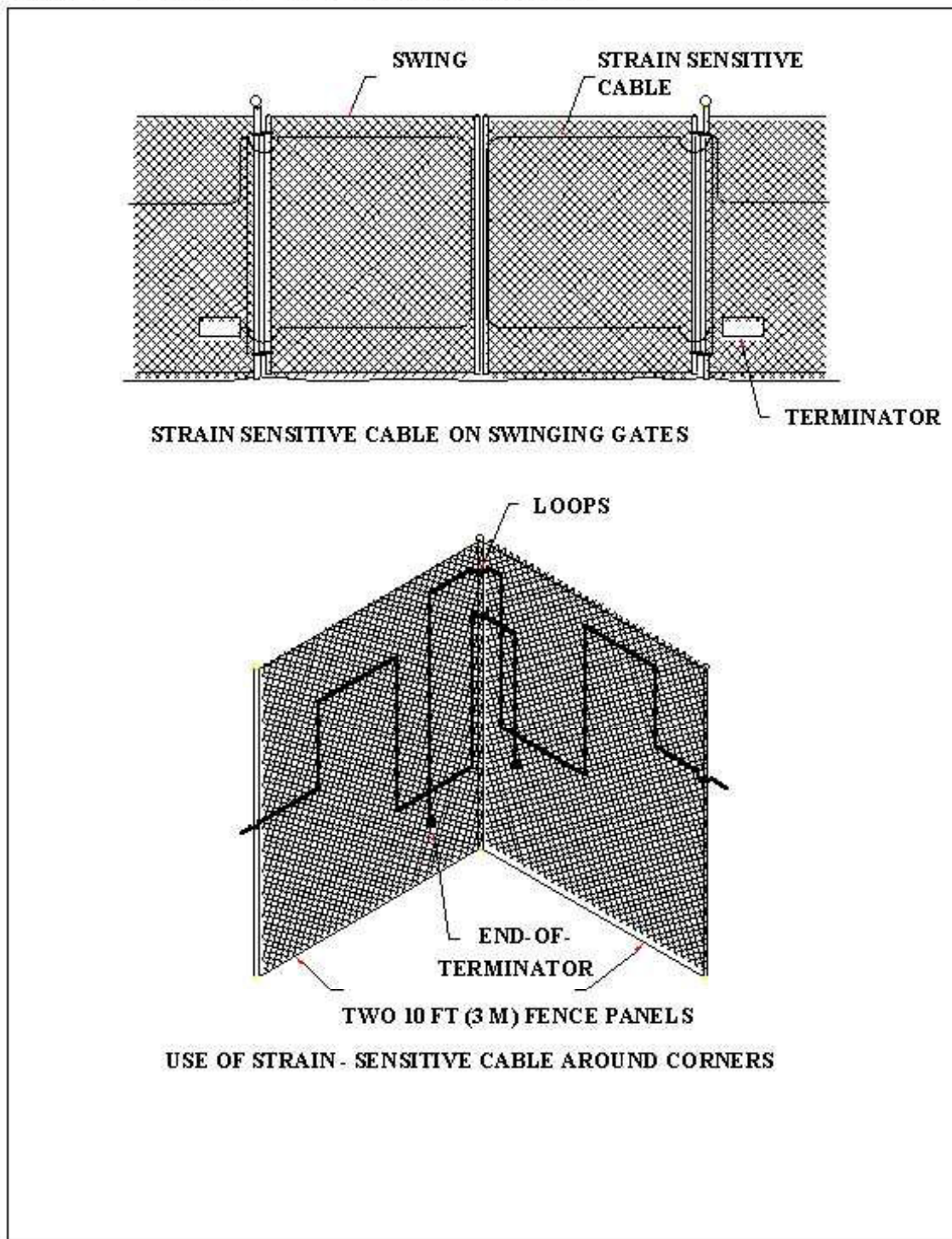


Figure LSS+4025 Strain-sensitive cable (applications)

### 40\_3.2.3C Fiber Optic Fence Sensors



#### LSS403: Fiber optic fence sensors

Fiber optic sensors use light rather than electricity as a carrier for transmission and detection. Fiber optic cable can be easily incorporated into existing fences, or it can be used as stand alone fencing.

The construction of an optical fiber is a thin strong strand of glass or other optical medium, often referred to as a wave guide because the optical fiber guides light waves from a light source to a detector at the terminating end of the fiber. Pulses of light replace their equivalent electrical impulses in a wire. There are many advantages over other conductive medium, including:

- **Immunity to electrical interference and Electrical Magnetic Interference (EMI) disruption;**
- **Intrinsically safe;**
- **High reliability due to the stability of the electronics;**
- **Greater transmission distances as compared to metallic carriers. Light has a very low attenuation factor through glass. There is approximately a 3db light loss (absorption) per kilometer.**

Based upon the signal processor, there are two primary types of fiber optic sensors: **continuity** and **microbending**.

The fiber optic continuity sensor requires the glass strand to be broken in order to initiate an alarm, and can be compared to a closed loop device. The transmission of light is monitored from source to receiver; a break in energy is detected as an alarm. A composite strand sensor can be combined with a continuity sensor contained within a barbed steel tape. An installed system is similar to a taut wire installation; the difference being that it does not require the mechanical activation of switches. This makes preventive maintenance and repair of the system more affordable. The tape can be used as a free standing fence or can be applied to an existing fence, or attached to walls and buildings.

The fiber optic microbending detects alterations in the light

pattern caused by movement of the cable, generally as the result of bending or distorted to affect the wave guide characteristics of transmission. This correlates to stress on the fence webbing. The cable is actually the sensor when it is integrated into the fence fabric. An LED provides the light source. A threshold of change in the transmission of light will provide an alarm.

In order to insure maximum reliability, sensors should be mounted directly on, or woven into, the fence fabric. As with all other fence line detectors, a quality and stable installation of the fence is necessary for reliable detection. The fence should be free of rattles, clanks, knocking sounds, and vibration and stress activity. This will maximizes line sensor quality. If there is significant ambient noise on or around the fence, the lower the sensitivity setting will be for the system, with the correlation that it will be less likely to detect an intruder. Supplementary sensors, such as in-ground, can add another level of protection. Volumetric sensors and video motion detection can also increase redundancy and security.

Unreliable detection will result from poor fence quality (stability). Loose fence fabric and poor stability cause the sensitivity setting for the fence to be calibrated lower than preferred, making the system less likely to detect an intruder. When properly installed on a good quality, stable fence or installed in a taut wire-like configuration, the system is very stable and reliable.

Nuisance and false alarms can be caused by extreme weather turbulence that damages or disturbs the fiber, or by animals. The system will not respond or be affected by transient voltage or lightning strikes, but can be affected by RFI, EMI, and extreme changes in temperature and blowing debris.

#### **40\_3.2.3C.1 Defeating Fiber Optic In-Ground or Fence Mounted Systems**

Fence protection systems that utilize fiber optic sensors, either mounted on the fence itself or in the ground, can be defeated. Techniques include:

- **Bridging;**
- **Tunneling under a barrier-mounted system;**
- **Careful and assisted climbing over a rigid turn or corner points in a coverage zone. In such cases, sensor coverage will**

generally not be as sensitive on a fence-mounted systems;  
• Alarm stacking.

#### FIBER OPTIC CABLE

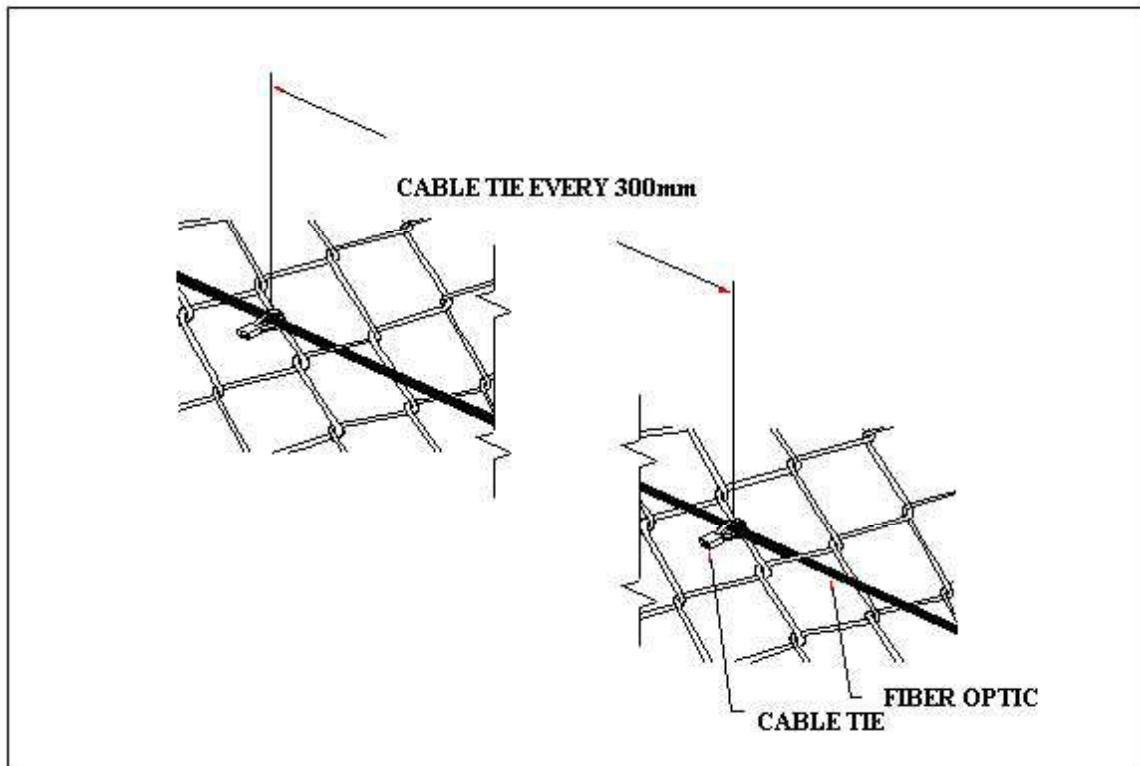


Figure LSS+4026 Fiber optic cable

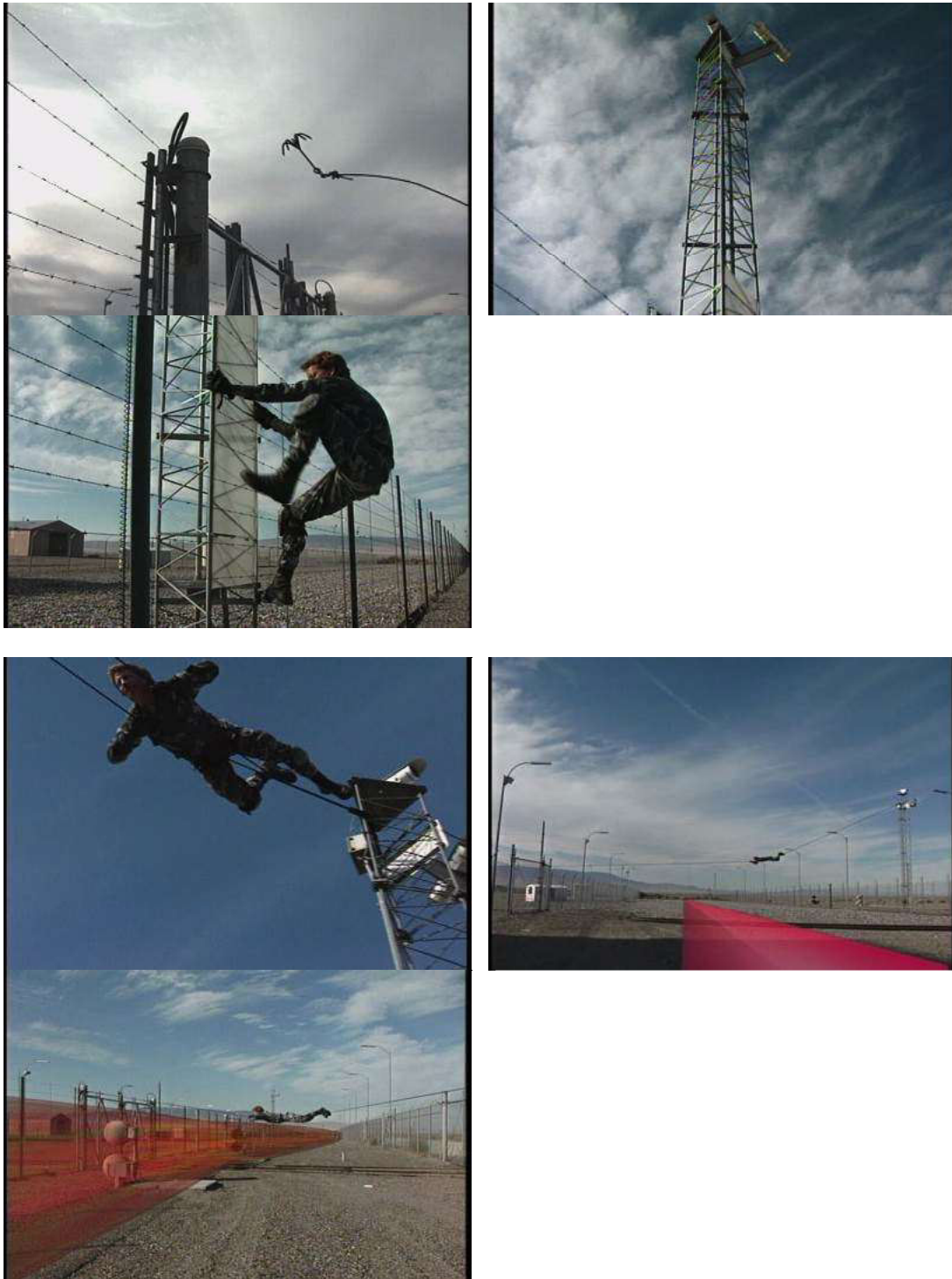
#### 40\_3.2.3D Defeat Techniques for Perimeter Fence Lines



LSS403: DOE on perimeter sensors and their defeat

Perimeter fence lines can provide the first barrier to entry by an intruder, although other sensors may detect a violation before the fence is reached. There are four recognized techniques for compromising fence lines and other perimeter sensors: **crawling, climbing, jumping, and bridging.**

##### 40\_3.2.3D.1 Bridging



**Figure LSS+4062 Bridging of the sensor is a popular method of bypass. In these photographs, simulation of a microwave path is shown in red. The intruder is able to bridge across and**

2459 22/09/2007 11:42:39 AM  
(c) 1999-2004 Marc Weber Tobias

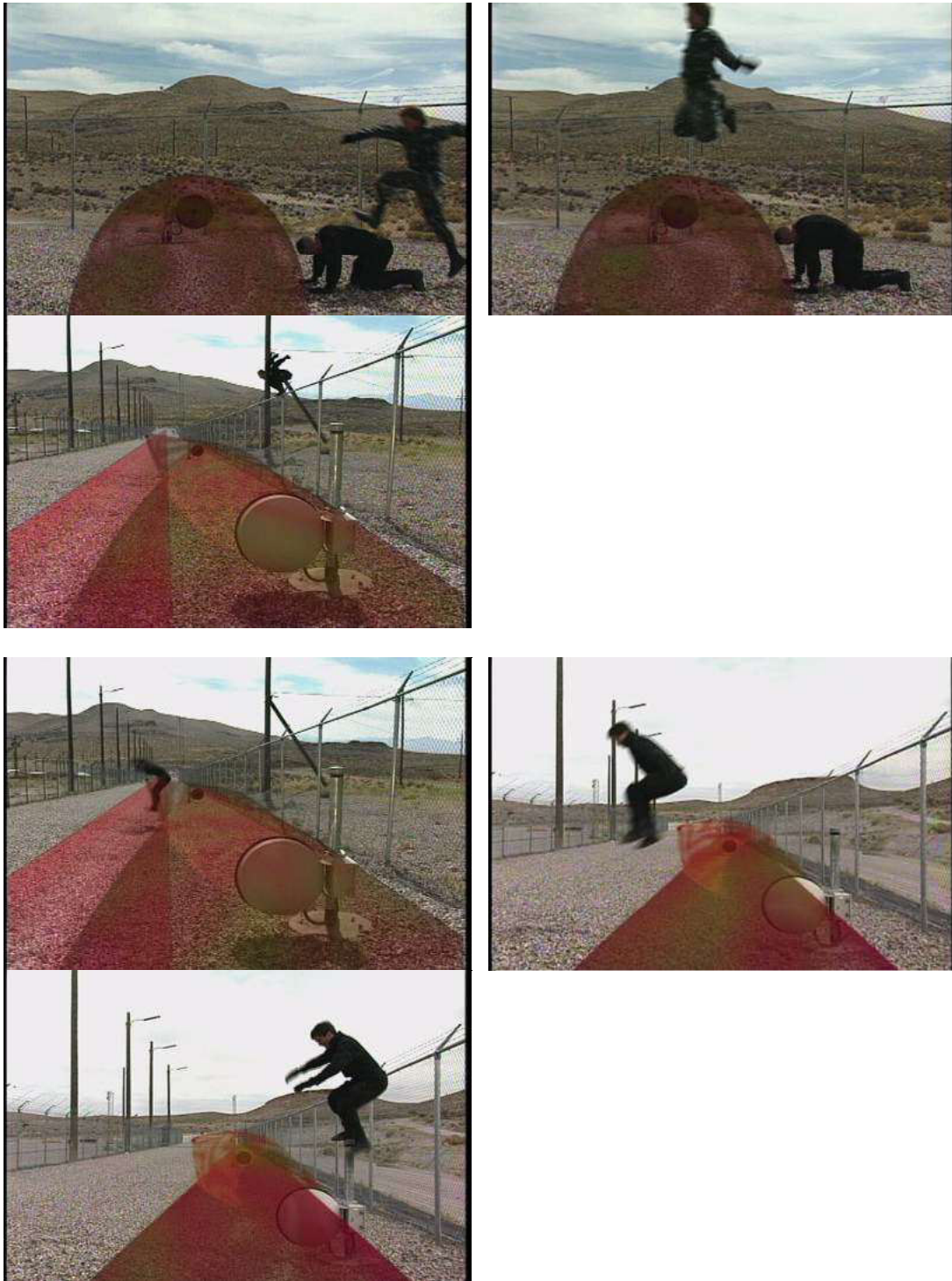


over the RF pattern, avoiding detection. Courtesy of DOE Office of Security and Safety Performance Assurance

#### 40\_3.2.3D.2 Jumping







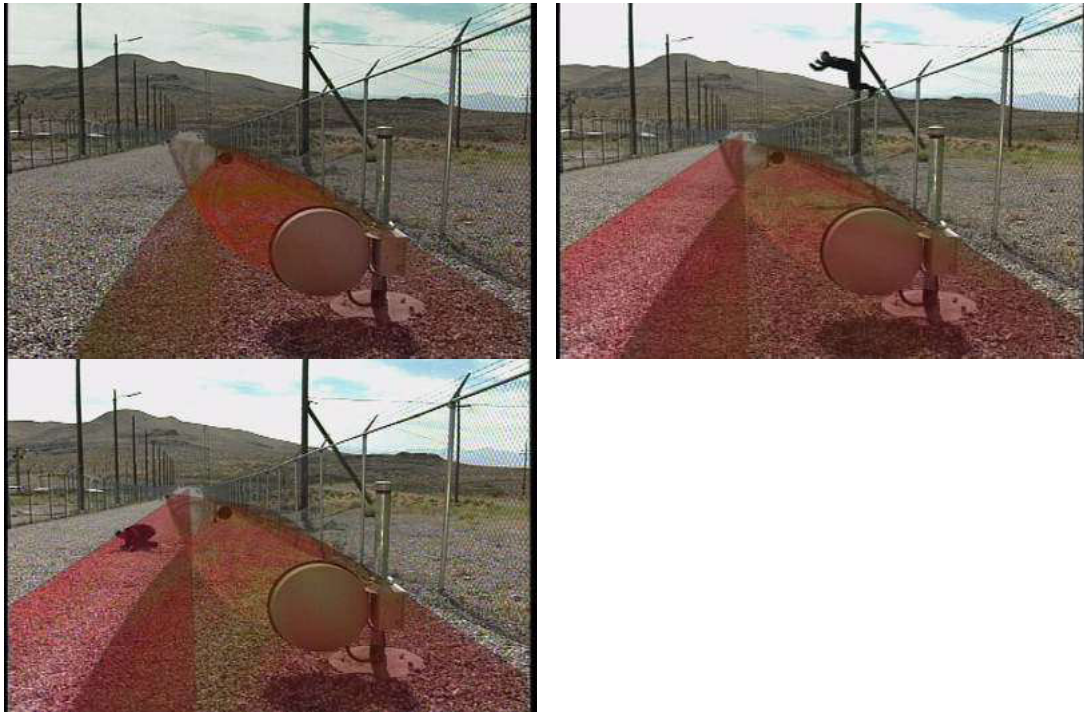


Figure LSS+4063 An intruder is able to successfully jump over a monostatic microwave pattern, but not for a bistatic system. Note the overlapping coverage that catches the intruder. Courtesy of DOE Office of Security and Safety Performance Assurance

#### 40\_3.2.3D.3 Climbing







Figure LSS+4064 A climber is able to scale a fence by gaining a foothold. This is poor design.



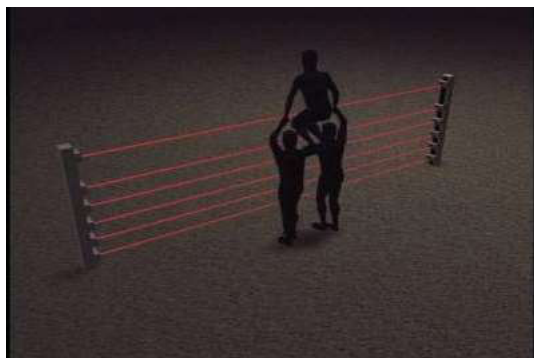


Figure LSS+4065 Intruders are able to penetrate a facility using a variety of techniques. Materials are removed from the fence and used as an aid to the climbing process. The top of the fence line can be used for support. A

2464 22/09/2007 11:42:43 AM

(c) 1999-2004 Marc Weber Tobias



three-man climb can be accomplished to jump over barriers, such as the photoelectric beams, as shown. Boards may also be used as ladders to scale the fence. Courtesy of DOE Office of Security and Safety Performance Assurance

#### 40\_3.2.3D.4 Crawling

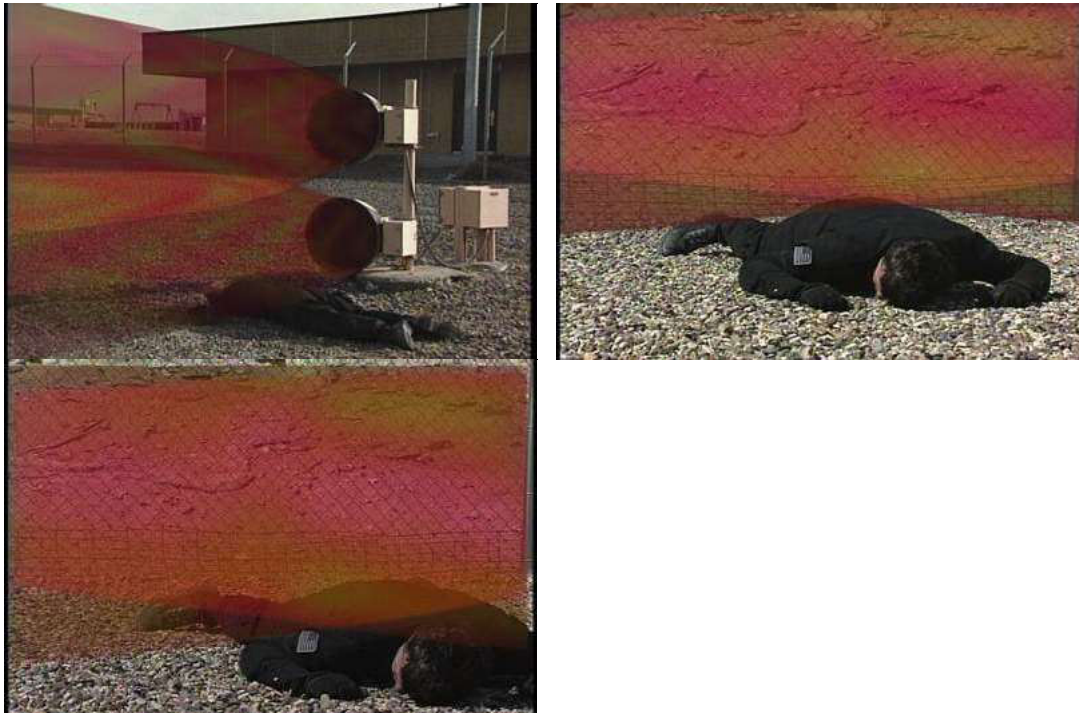


Figure LSS+4066 An intruder may crawl under or through sensor coverage. In the photograph, the intruder is able to circumvent a bistatic microwave system by passing under the RF field at an extremely slow pace. Courtesy of DOE Office of Security and Safety Performance Assurance

#### 40\_3.2.4 Wall Vibration

Vibration sensors are designed to be mounted on walls, ceilings and floors and intended to detect mechanical vibrations caused by chopping, sawing, drilling, ramming or any type of physical intrusion attempt that would penetrate the structure on which it is mounted. See the discussion in section 40\_3.2.3 above.

Transducers that are designed to detect the low frequency energy that is typically generated during a physical intrusion attempt and transmitted via the surrounding walls, roof or floor. The sensors are mounted directly to the inner walls of the protected zone, and will detect the change in the normal "vibration"



profile.

There are two basic types of transducers that are utilized to sense these changes: piezoelectric and mechanical transducers. Both devices convert the seismic shock waves into electrical signals that are proportional to the acquired energy. These are processed and analyzed against known signatures.

Reliable operation requires that sensors should be securely and firmly spaced from eight to ten feet apart on a wall or ceiling where intrusion is expected. Actual placement is dependent upon the transmission characteristics of the target wall. The use of sensors should be avoided on walls of limited structural integrity, such as sheet rock, plywood or thin metal, unless bolstered by main supports. These materials are subject to external vibrations other than caused by an intruder. Likewise, walls that adjoin or are exposed to vibration created by trains, planes, trucks, or vibrating machinery should be avoided.

Supplementary detectors are recommended for added reliability of detection. Volumetric or infrared sensors that focus on vulnerable areas will increase security.

Problems can result from the improper placement of sensors, or their application to inappropriate surfaces. Erratic operation can result from:

- **Unstable or improper installation of units;**
- **Improper spacing of units;**
- **Mounting of the sensors to materials (rugs, fabric, heavy wall coverings) that are not conducive to detecting vibrations;**
- **Poor placement of sensors;**

These sensors can be bypassed by:

- **Avoiding entrance through the protected area;**
- **Selection of a point and method of entry in a segment of a wall, roof or floor that will permit the suppression or diffusion of vibrations created by the entry;**
- **Generation of a persistent but random number of false alarms over a long period of time.**

## WALL VIBRATION SENSOR

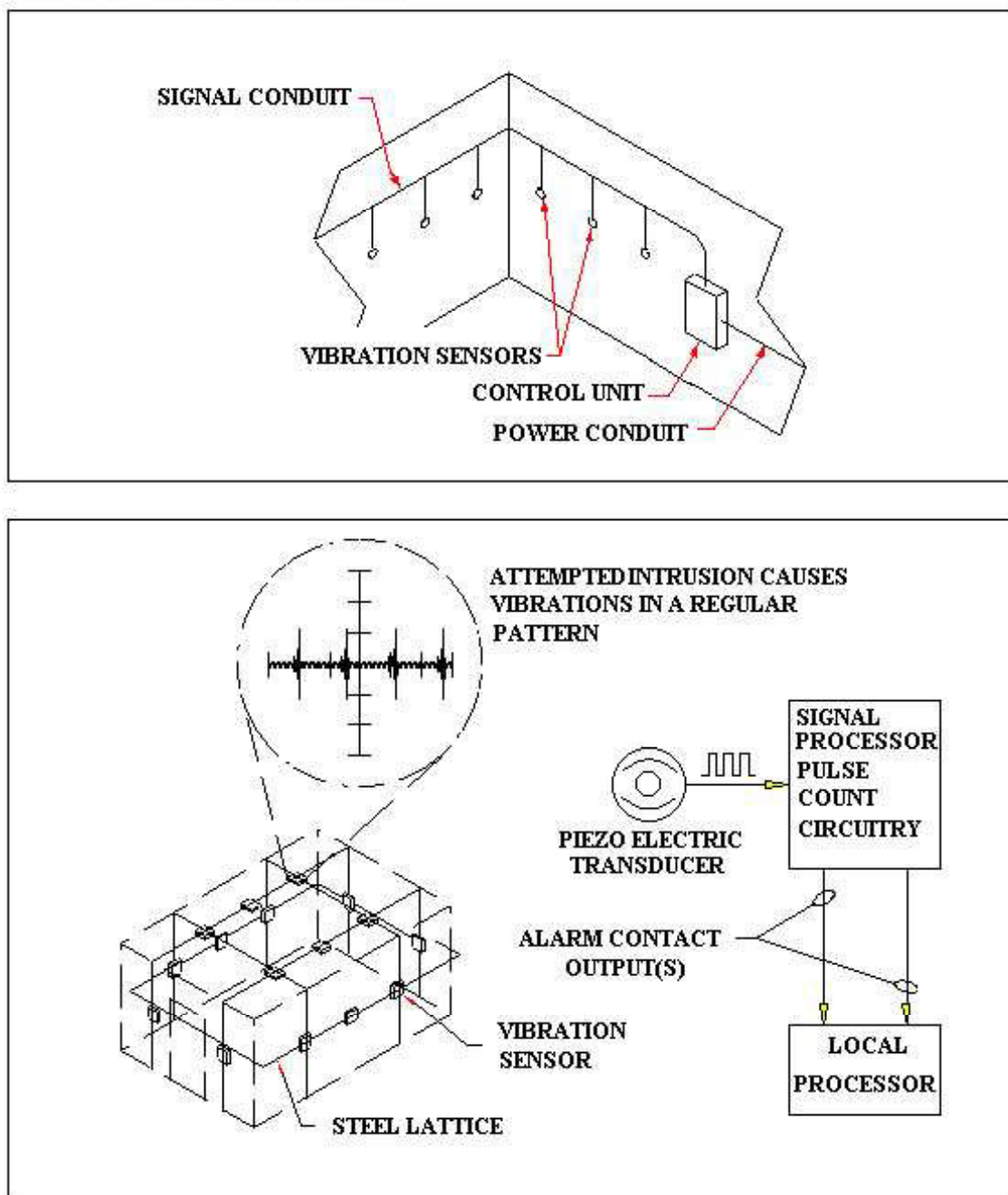


Figure LSS+4009 Wall vibration sensor

### 40\_3.2.4.1 Defeat of Wall Sensors

Fiber optic wall sensors can be defeated by:

- **Avoidance;**
- **Targeting an insensitive or overlooked location as a point of entry;**
- **Bypass the sensor circuit while the system is disarmed.**

#### **40\_3.2.5 Fiber Optic Wall Sensor**

This type of sensor is configured as an open mesh network (quilt) appliqué that can be applied directly to an existing wall or roof, or installed in a wall (or roof) during construction. The system is designed to sense vibrations at low frequency energy that are created by chopping, sawing, drilling, ramming or other physical attempt to penetrate the structure on which it is mounted. This detection is similar to other fiber optic devices described in this text. There is a source LED that generates light through the fiber, and received by a detector that is sensitive to changes in the transmitted energy. Signatures of various low frequency components are stored within the processor and matched to minute variations in transmitted energy.

Fiber optic wall detectors are extremely sensitive and are not suitable for every installation. They should not be installed on any wall or surface that is exposed to external vibrations, such as generated from aircraft, vehicles, trains, or machinery. They should not be used on walls of poor structural integrity, such as sheet rock, plywood or metal. Smart processors can be programmed for differing types of intrusion, but cannot distinguish between certain external stimulus.

As with other vibration detectors, unreliable operation will result if they are installed or calibrated improperly, or implemented on surfaces that are unsuitable. These systems can be compromised by an intruder avoiding entry through a protected area, or penetrating an insensitive location.

### FIBER OPTIC STRUCTURAL VIBRATION SENSOR

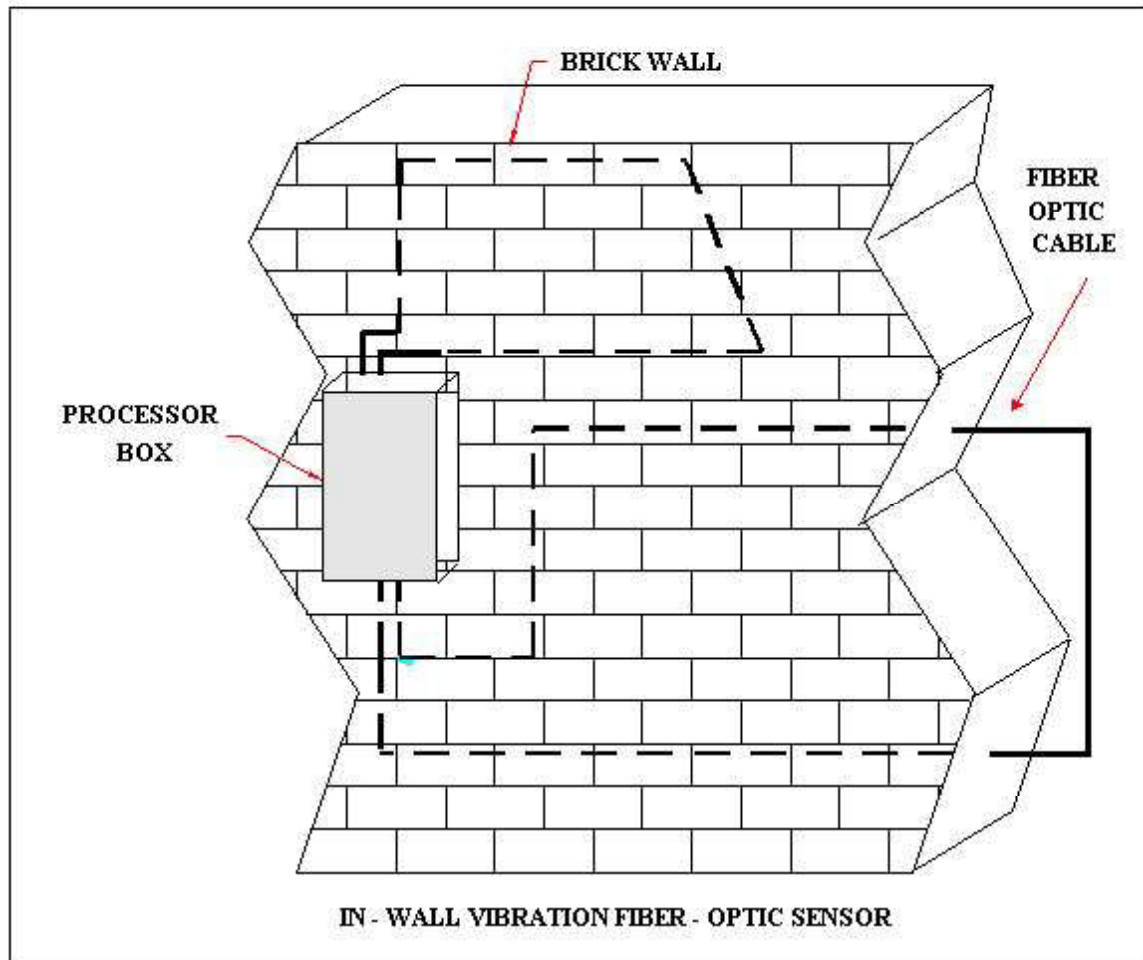


Figure LSS+4010 Fiber optic structural vibration sensor

#### 40\_3.2.6 In-Ground Fiber Optic Sensor

Fiber optics can also be used for an in-ground, pressure sensor. The theory of operation is similar to most other light emitting devices described in this text. A light source provides an emitter at one end of the glass network. The conductivity and reflectivity of the system is calculated, and the energy at the receiving sensor is constantly evaluated. Pressure on the cable can create changes in the characteristics of the received signal. Such pressure can be caused by vibrations from walking, running, crawling or jumping.



These systems should not be installed near poles, trees, in or under concrete or asphalt. If they must be located near a pole, then the protected zone should be at a distance equal to the height of the pole. The area of installation should have proper drainage in order to prevent water from collecting over the detection zone.

There are several conditions that will create false alarms when using in-ground fiber optic sensors:

- **Areas with erosion problems caused by heavy rain or lack of vegetation. This can result in the cable being exposed or buried deeper in the earth, causing any sensitivity settings to become ineffective;**
- **Tree roots can be affected by windy conditions above ground that can cause their movement underground and result in bending of the cable;**
- **Large animals passing over the zone of protection.**

These systems can be defeated by bridging over the sensor area. Because of this, supplementary sensors such as microwave are recommended.

## IN-GROUND FIBER OPTIC SENSOR

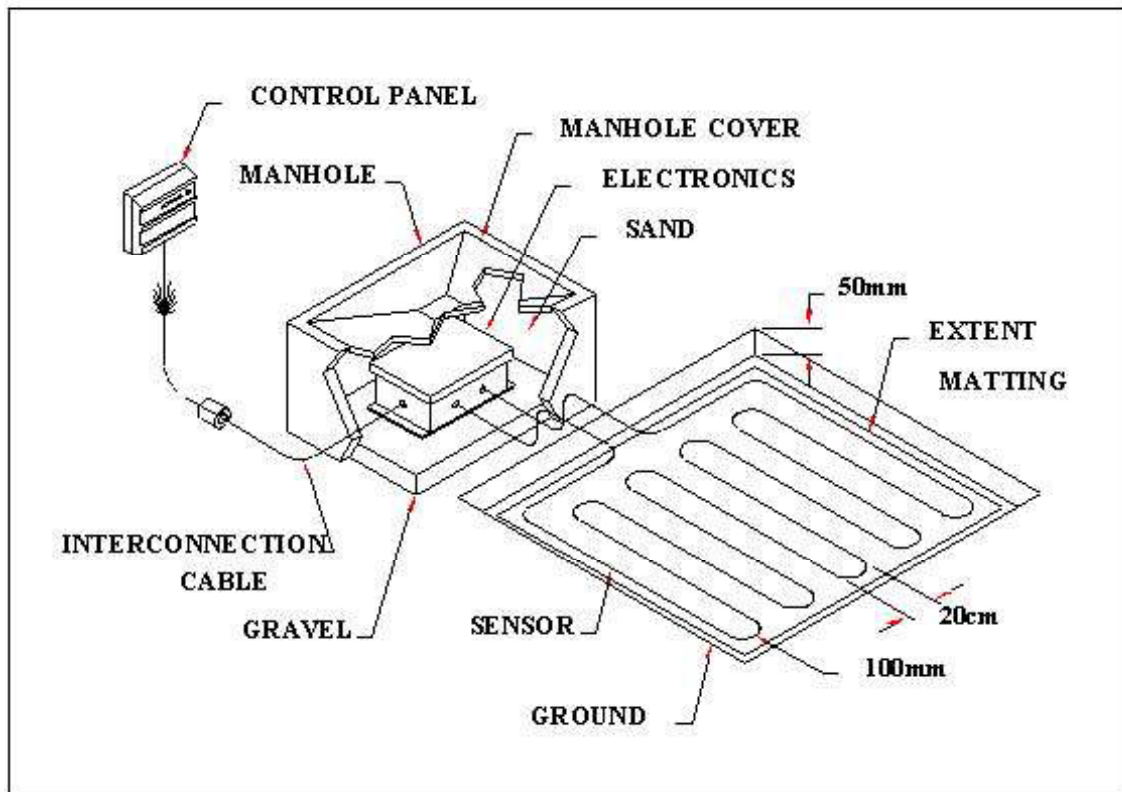
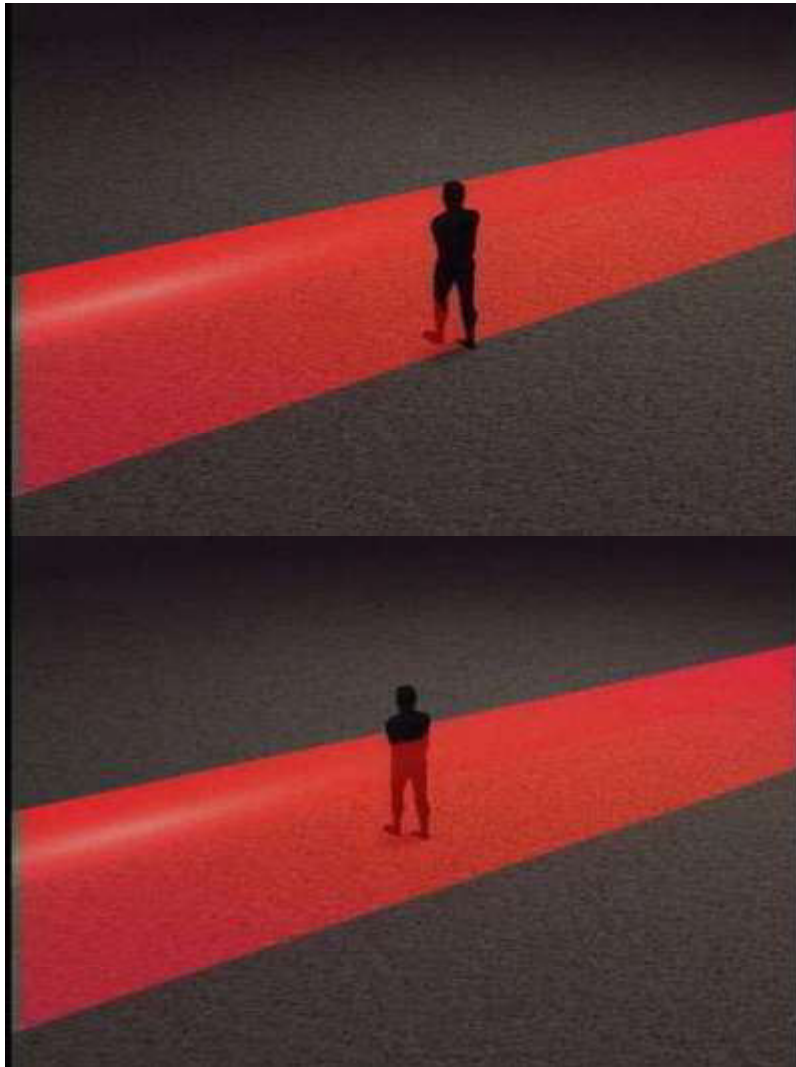


Figure LSS+4030 In-ground fiber optic sensor

### 40\_3.2.7 Ported Coax Buried Line



LSS401: Buried Cable sensors



**Figure LSS+4060 Ported coax emits an RF field above the cable that can detect an intruder as the beam of energy is crossed. Courtesy of DOE Office of Security and Safety Performance Assurance.**

Ported coax buried line sensors are coaxial cables that have small, closely spaced holes in the outer shield that allow electromagnetic energy to escape and radiate a short distance. This emission creates an electric field that can be disturbed upon the presence of an intruder. The system requires that cables be installed in pairs spaced about five feet apart. Under the control of a central processor, a pulse of radio frequency energy is transmitted through one of the cables and received by the other. The pulse timing is constant and thus creates a signature that can be constantly evaluated by the processor. Any

interruption of the field will cause a change in this signature that can indicate an intrusion. The processor has the intelligence of updating its signature parameters to adjust for gradual changes in the environment and surrounding medium.

There are two basic types of sensors: **continuous wave**, and **pulsed**.

A constant emission of RF energy is transmitted simultaneously through the **continuous wave** sensor in both cables and received by the opposite number. This creates a detection zone above ground with a continuous surface. When an intruder enters this area, the electric field is disturbed.

**Pulsed sensors** emit a pulse of RF energy through one cable and receive it through its corresponding receive side. As the transmission speed is constant, this creates a standard amplitude signature that can be evaluated.

The cables are typically buried about nine inches below the surface of the ground, depending upon the soil density. This creates an electric field that is approximately three to four feet above the ground and extends nine to twelve feet in width. The variation in zone size depends upon cable separation and the characteristics of the burial medium. Using this sensor, zone length can extend up to five hundred feet.

Routing of cables underneath chain link fences, or running metallic pipes through the sensor field should be avoided. If this is impossible, they should be buried at least three feet below the ported coaxial cable. When installing the cables along or near fence lines, the cables must be installed between six and ten feet from the fence in order to avoid distortions and to reduce potential false alarms that can be caused by the motion of the fence fabric disrupting the detection field. Supplementary protection in the form of video motion detection can complement the cable sensor system.

Ported coaxial systems can suffer from false alarms and unreliable operation if installed incorrectly or in difficult environments, such as where there are nearby metallic fence fabric, vehicles, signs, and organic objects such as people, medium to large animals, and medium to large vegetation. Although individual small animals generally do not have the mass to affect these systems, a congregation of small animals can cause distortions.

Heavy snowfall can cause problems due to the limited height of the detection zone. In addition, burial mediums that have drain ducts located beneath the buried cables, and wind disturbance of standing water over the cables can pose a problem. In such cases, ducts must be constructed of metal. The burial zone should be graded to provide immediate runoff and good drainage. It should also be noted that ported coax sensors are affected by high EMI from sources such as large electrical equipment or electrical substations and should not be used in close proximity to these types of installations.

#### **40\_3.2.7.1 Defeating Ported (Leaky) Coax Cable Systems**



2474 22/09/2007 11:42:44 AM  
(c) 1999-2004 Marc Weber Tobias



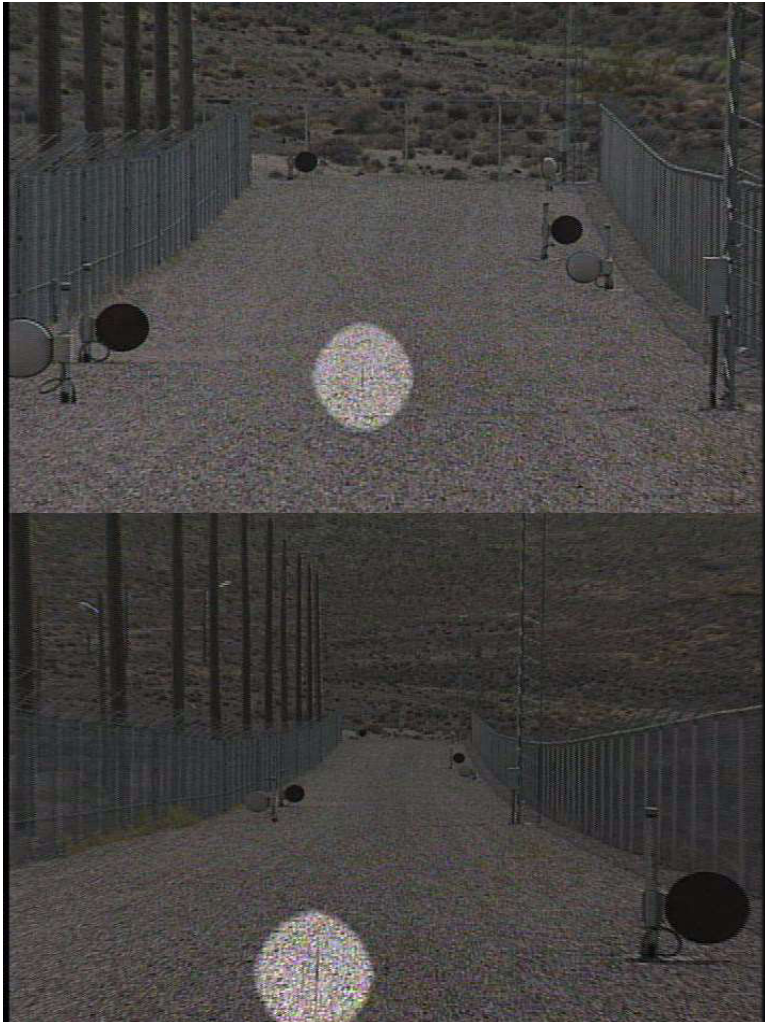


Figure LSS+4055 Marker points for buried coax systems should be removed because they provide an indication of coverage for an intruder. Courtesy of DOE Office of Security and Safety Performance Assurance.

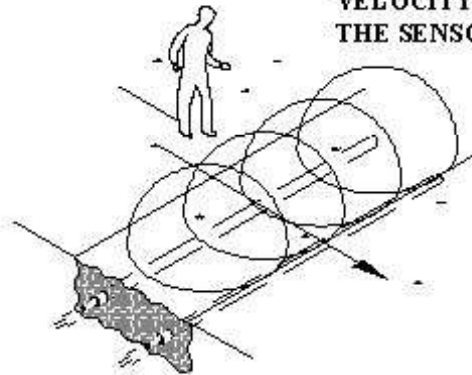
Perimeter defense systems that utilize ported or leaky coaxial cable can be defeated through a variety of methods. These include:

- Walking on wooden stilts;
- Bridging, two-man or pole vaulting over the detection zone;
- Alarm stacking;
- Leaching a salt water solution slowly through the cable in a specific zone over a period of time. This procedure will have the affect of desensitizing the sensor cable;

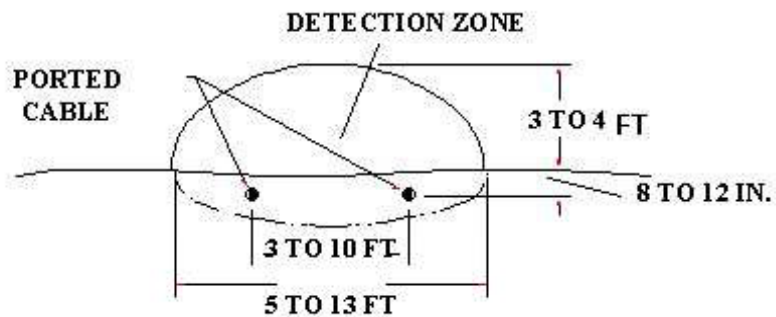
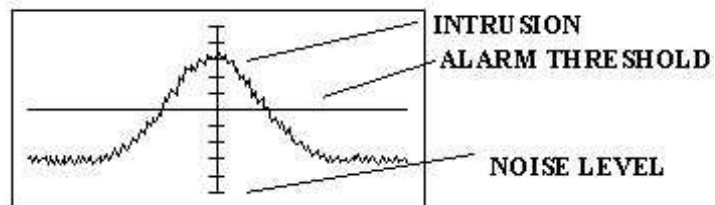
- Cut the cable from the fence to create an intrusion path;
- Bypassing the area of coverage;
- Using marker points as an indicator of coverage.

## BURIED PORTED CABLE SENSOR

BURIED PORTED CABLE SENSOR  
RESPONDS TO INTRUDERS MASS AND  
VELOCITY IN MOVEMENT THROUGH  
THE SENSOR FIELD.



BURIED PORTED CABLE SENSOR SIZE AND SHAPE  
OF DETECTION PATTERN IS DEPENDENT UPON  
CABLE SEPARATION, BURIAL DEPTH, AND SOIL  
CONDUCTIVITY LEVELS.



**Figure LSS+4031 Buried ported cable sensor**

#### **40\_3.2.8 Balanced Buried Pressure Sensor**

A Balanced Buried Pressure line sensor is another type of in-ground system that detects vibrations and seismic energy that can be caused by personnel, animal or vehicular movement across the surface of the ground in which the sensors are installed. The tubes are extremely sensitive to pressure changes upon the medium in which they are located. Ground within a zone that is subjected to walking or running intruders, vehicles, or other forms of compression will cause proportional changes in pressure in the farthest tubes. This is processed and analyzed.

The amount of sensed pressure waves directly relates to the weight and movement impact that is created by objects contacting the earth. Each type of impact creates its own identifiable signature, much like sonar. Thus, a runner will create greater pressure than a person that is walking. Likewise, a heavy person that is walking upright will create more pressure than a smaller person moving on hands and knees.

Sensor zones (usually two sensor tubes) consist of pressurized, closed end, pliable tubes or hose segments filled with water or an antifreeze-like solution. The zone size will vary depending upon soil density and composition and the nature of any surface material. The tubes are very sensitive to changes in pressure and react to pressure exerted on the medium in which they are implanted or buried. A processor monitors and regulates the pressure inside the tubes and generates a signal if there is a deviation from a determined norm.

There is a self-compensating valve that is used to maintain pressure within the tubes, and to adjust to gradual or moderate (not rapid) changes that can be associated with the burial medium (not of personnel and vehicle movement and other man-made or sudden natural movements such as earthquakes and explosives). Such changes might include those caused by moisture content (rain) or temperature changes (frost or drought). The differential pressure system and the nature of the self-compensating valve provides a high degree of immunity to normal environmental noise and weather conditions.

A detection zone is created by burying the tubes approximately four feet apart, with the pressure-sensing unit linked and placed between the sensor tubes. Depending upon the nature of the soil,

this type of system can create a detection zone that measures up to a 350 feet radius. The depth at which the tubes are placed depend upon the composition of the medium in which the tubes are placed. Depth for different medium is as follows:

- **Earth and sand: ten inches is sufficient;**
- **Soil with an asphalt covering: four to eight inches;**
- **Concrete surface or area: bury just beneath the under-surface of the concrete, because this material is not a good conductor for waves created by personnel. It serves to dampen or insulate such waves, thereby reducing the probability of detection.**

Tree roots closer than ten feet to a sensor set can pose a false alarm problem, due to the potential for windy conditions above ground. Such movement can transfer pressure waves into the ground via the root system. So also, areas with heavy snowfall or shifting sand may create a problem for the system to properly sense seismic vibrations. In such cases, snow and sand look the same to detectors with respect to the shock waves created upon their movement. This would, of course, depend in part on the depth and composition of the snow or sand.

As with other systems discussed above, the improper installation or calibration of detectors can cause normal activity to be interpreted as an alarm condition. The location near heavy road or rail traffic or seismic activity from pulsating or shock machinery can generate nuisance alarms.

#### **40\_3.2.8.1 Defeat of Balanced Pressure Sensors**

The ability to defeat these systems relies upon the avoidance of potential zone(s) of detection or of the following actions:

- **Cushioning movement vibrations;**
- **Dispersing or a lowering of impact energy;**
- **Attacking the sensor in extremely cold weather;**
- **Alarm stacking;**
- **Avoidance of sensor;**
- **Bridging or planking over or through the detection zone.**



### BALANCED BURIED PRESSURE LINE SENSOR

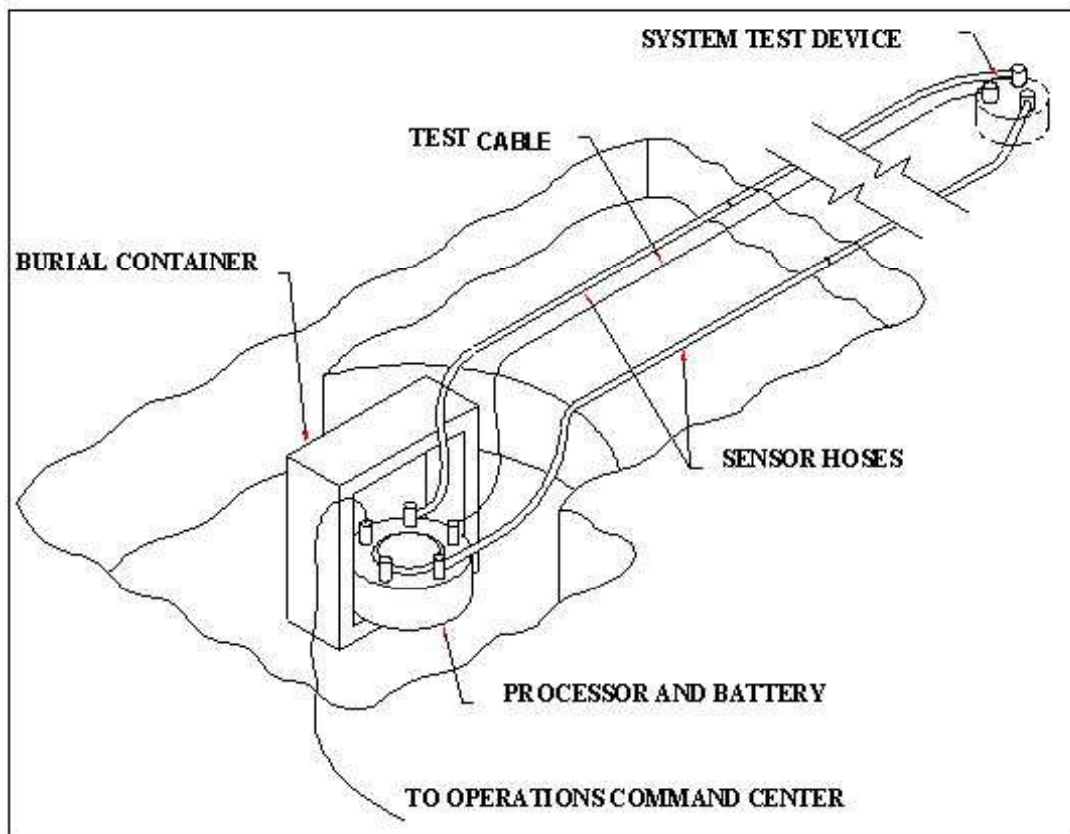


Figure LSS+4032 Balanced buried pressure line sensor

#### 40\_3.2.9 Buried Geophone

A buried geophone transducer is designed to detect the low frequency seismic energy created in the ground by someone or something crossing through the detection screen above the sensor by crawling, walking, or running.

The system consists of two elements, a processor and a series of geophone sensors. Signals are generated by the detectors that are then filtered and processed, based upon predefined signatures. In typical installations, twenty to fifty geophones are placed in a line of detection that can extend up to three hundred feet. They are buried between six and twelve feet apart to a depth of six to fourteen inches in soft to compact soil, and six inches in asphalt. Soil must be stable and relatively compact, with the geophones seated between layers of sand, due to its conductivity.

In many systems, direct audio monitoring is available to validate alarms by human operators. Much like Sonar in a submarine, a trained operator can usually differentiate between normal stimuli and that associated with intrusion attempts.

These systems are subject to unreliable detection and false alarms if the material in which the sensors are buried is inconsistent or loose. In such cases, the soil becomes a poor conductor of energy, resulting in little data being received by the geophone. On the other hand, the detectors are sensitive to low levels of seismic activity and thus, noise can be generated by animals, trees, fences, light poles and telephone poles. Each of these structures are anchored in the ground and are conduits for energy transfer. Because of this, a geophone should be located at least thirty feet from a tree, ten feet from any fence, and at a distance equal to the height of any nearby pole.

Geophones, as with all vibration detectors, can be defeated by bridging over the sensor.

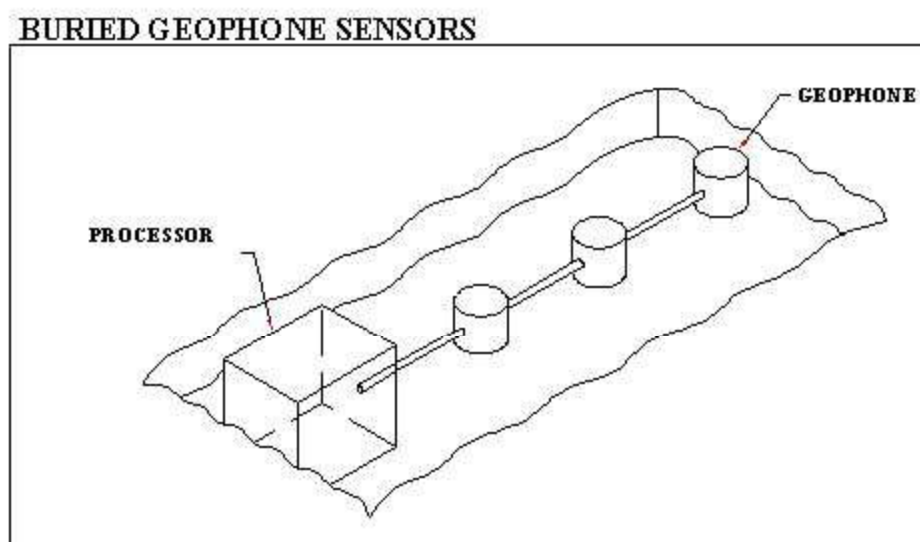


Figure LSS+4033 Buried geophone sensors

#### 40\_3.2.9.1 Defeat Techniques for Geophone

Sensors that detect vibration or seismic energy (geophones) can be defeated through a variety of techniques, including:

- **Bridging;**

- Tunneling under the sensors, or use of a two-man pole vault over the fence-mounted version;
- Stacking of alarms;
- Avoidance;
- Explosive penetration if pulse count is set improperly;
- There is a high probability of alarms during storms or wind. This fact can be used to bypass a system by creating trips that may be ignored;
- Spoofing and alarm stacking.

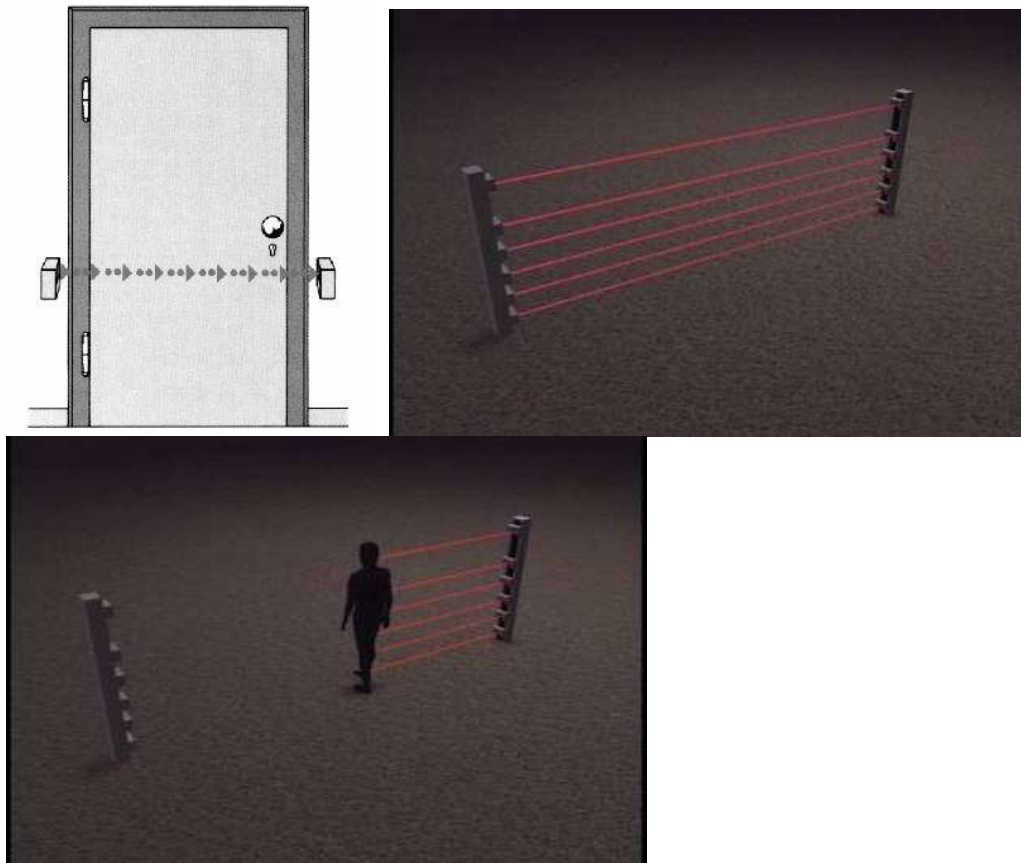
### 40\_3.3 Light-Activated Sensors



#### LSS401: Photoelectric sensors

Light sensors are employed to provide an invisible electronic barrier against entry. They can be positioned within a building or outside along a perimeter to protect a path against intrusion. Photoelectric sensors transmit a beam of infrared light to a remote receiver and thereby create an "electronic fence". Such sensors can "cover" openings such as doorways, walls, or hallways; they act like a trip wire. Once the beam is broken or interrupted by an intruder, a contact closure or other signal is generated. Photon-sensitive devices rely upon the transmission and interruption of one or more light beams for their operation. When photoelectric systems are installed properly, they will provide a reliable measure of protection for small or large areas.

A system consists of a transmitter and receiver. The transmitter emits one or more narrow light beams in a straight or reflected path to the receiving unit for a range of up to 1,000 feet. So long as the rays are not interrupted, the receiver will maintain a continuous circuit.



Photoelectric sensors are comprised of two critical components: a **transmitter** and a **receiver**. The transmitter utilizes a Light Emitting Diode (LED) as its light source. It generates a consistent infrared beam to a receiver. The receiver is actually a photoelectric cell that detects the presence of IR at a specific modulated frequency. If the detector fails to receive at least 90% of the transmitted signal for as brief as 75 ms.(time of an intruder crossing the beam), an alarm condition is created.

In most systems, the IR carrier (one or more beams) is modulated at a very high frequency, and this frequency is further changed at a rate of up to 1,000 times per second in an algorithm that correlates with that programmed into the receiver. This prevents bypass attempts through the use of a substitute light source. The only way to bypass this system would be to replicate the angle of the beam and modulation frequency.

In practice, the transmitter and receiver can be separated up to 1,000 feet and still provide reliable coverage. A photoelectric sensor is not affected by changes in thermal radiation,

fluorescent lights or Radio Frequency Interference (RFI). These systems exhibit a high probability of detection and low false alarm rate. The path of the beam can be altered using mirrors to create a less predictable detection barrier, although the use of mirrors can reduce the signal strength of the beam and diminish its effective distance. If mirrors are utilized, caution must be exercised because they are often accidentally knocked out of alignment, generating a need to calibrate and realign them periodically. They are also prone to dust build-up and refraction or diffusion of the reflected beam.

The major failure in these systems is the introduction of anything that blocks or interrupts the path of light between transmitter and receiver. Such action can affect the detection reliability of the sensor. Fog, smoke, mist, dust, and reflective particles cause the light to be refracted or scattered. If there is more than 10% reduction in the signal strength, an alarm is normally generated. Extreme variations in background lighting or sunlight may also reduce sensitivity.

A nuisance or false alarm can be caused by any objects that interfere with beam transmission, such as birds, animals, blowing leaves, or paper. The improper alignment of the transmitter, receiver or mirrors can also generate an alarm.

#### **40\_3.3.1 Defeat of Light Sensing Systems**

**Light level** detection systems are triggered by the presence or absence of ambient light. They differ from photoelectric sensors in that they sense lighting conditions, rather than a specific directed beam across an identified path. Light sensing systems can be neutralized by:

- **Entry without alteration of the ambient light level;**
- **Use of night vision devices in an optically controlled environment;**
- **Blinding of the light sensor to simulate a specific condition;**
- **Blocking of sensor to prevent the detection of light. The photograph shows the use of black electrical tape to defeat a light level sensor at the diamond exchange in Antwerp, Belgium during a large burglary.**





#### **40\_3.3.2      Defeat of Photoelectric Active Infrared Sensors**

There are several techniques for defeating internal and perimeter photoelectric detection devices. These include:

##### **Interior Sensors**

- Avoidance, moving or stepping over or under the sensor light beam or projected laser plane, by determining the location of transmitter/receiver or reflective tape. Proper placement of mirrors can counteract this vulnerability by creating a "zig-zag" multiple beam barrier pattern;
- Extension of fiber optic cable material from transmitter to receiver in order to create a new light path;
- Capture of a beam by external light source. This will generally apply to non-pulsed units using visible light only, although modulated IR or lasers may also be utilized;
- Interposing reflectors or mirrors in a single-ended systems (Bounce back);
- Spoofing and alarm stacking;
- Using a black and white camera or IR goggles to determine light source;
- Stacking of alarms using birds;

##### **Exterior Sensors**

- Tunneling or trenching under the sensor beam pattern;
- Bridging, two-man or pole vaulting over the sensor beam pattern;
- Beam capture of unmodulated sensors only;
- Avoidance of the sensor, by stepping or sliding through improperly spaced beams;

- Utilize the ridged sensor sunshades or the sensor itself as a ladder. This is model dependant;
- IR beams can be observed by using a monochrome CCTV camera or IR goggles to determine transmitter path;
- Alarm stacking using another IR light source aimed at the receiver.

## 40\_3.4 Proximity and Capacitance Sensors



### **LSS402: Proximity sensor technology**

Proximity detectors can signal the presence of intruders near to or touching a certain object or area by a change in capacitance, inductance or other characteristics of the structure. They are used in driveways, office areas, schools, banks, strong rooms, safes, and other locations where specific structures or items are to be monitored.

Magnetic point detectors are utilized to sense large metal objects such as vehicles driving across concrete.



### **LSS403: Magnetic point sensors**

Capacitance sensors are designed to detect changes in an electrostatic field that is created by an array of wires. The presence of an intruder can change the capacitance of the field by approaching or contacting the wires. The sensors consist of three closely-spaced wires that are arrayed and installed on the top of a fence. A low voltage signal is induced in the array that creates an electrical field, utilizing the fence as the system electrical ground. A processor continually measures and compares the differential capacitance between the sensing wires and ground.

Three strands of closely spaced 16 gauge wire form the sensor array. The wires are secured to a fence top fabric or wall by using high-dielectric brackets, which can be adapted to any barrier. They are most commonly utilized on outriggers atop chain link fences. The sensor segment can extend 1,000 ft. In order to trip the sensors, physical touching of the fence is usually required. If the sensitivity of the system is increased, then close proximity can often trip the system. Supplementary sensors should also be installed, because these systems are subject to bypass by cutting of the vertical fence fabric. The systems are

2486 22/09/2007 11:42:47 AM

(c) 1999-2004 Marc Weber Tobias

impervious to weather, EMI, and RFI; such conditions have no effect on detection capabilities, although there is a high level of maintenance required to assure that the capacitance characteristics of the fence are always adjusted.

False alarms or unreliable detection can occur from vibrations caused by weather and animals (birds, squirrels and others). Vegetation coming into contact with the fence can also change the capacitance, thereby affecting the detection characteristics. Proper landscaping maintenance of the fence line must be insured (grass cut, trees removed, shrubs removed). Blowing debris or anything making physical contact that changes the characteristics of the fence can create an alarm condition. One countermeasure for this problem is inducing tension with springs at the termination points.

#### **40\_3.4.0 Defeating Proximity and Capacitance Sensors**

Capacitance and proximity sensors can be defeated by a number of techniques, including:

- **Disconnection from protective detection loop while the system is disarmed. This will be effective in self-balancing systems only;**
- **Use of insulating blankets, rubber wet suits, or gloves to prevent shorting of the capacitance field to ground;**
- **Bypass the sensor circuit while the system is disarmed;**
- **Tunneling or bridging of the sensors.**

Differential Capacitance Systems, utilized in exterior applications, can be defeated by:

- **Tunneling under the sensor or barrier (such as a fence);**
- **Bridging, two-man or pole vaulting over barrier;**
- **Wearing heavy insulated clothing, gloves or other material;**
- **Alarm stacking;**
- **Avoidance by attacking or penetrating the location at gaps in the sensor coverage;**

Magnetic point and driveway alert sensors can be defeated by:

- **Bridging, two-man or pole vaulting over detection zone;**

- Use of wooden stilts;
- Intruders do not have any metal;
- Avoidance;
- Alarm stacking.

### CAPACITANCE SENSOR APPLICATIONS

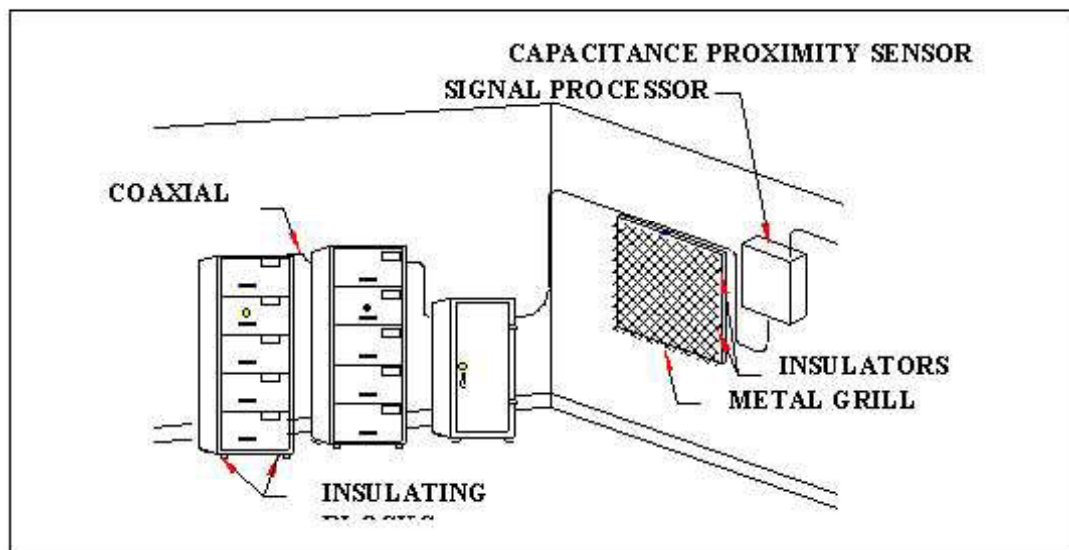
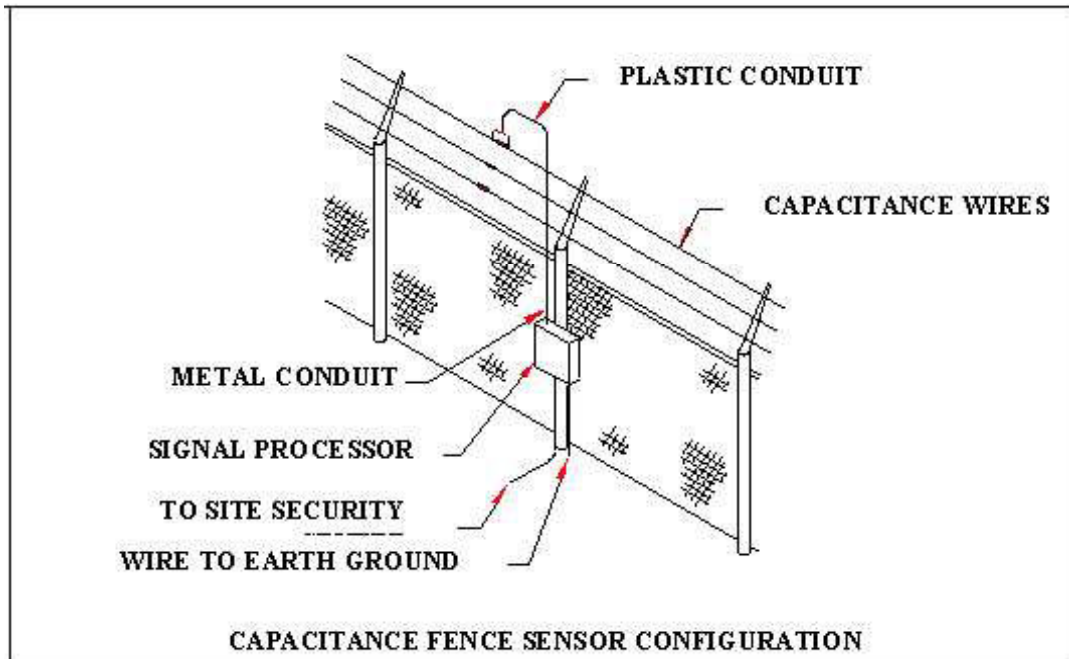


Figure LSS+4022 Capacitance sensor applications

#### 40\_3.4.1 Electric E-Field Sensor



LSS401: E Field protection







**Figure LSS+4048 An E field system by Siemens creates an electronic barrier through a series of parallel wires across the fence line.**

Electric field sensors are designed to generate an electrostatic field between and around an array of wire conductors and an electrical ground. Sensors detect changes or distortion in the field which can be caused by anyone approaching or touching the fence. Sensor zone length can extend up to 1500 feet.

The E-field sensor consists the following components:

- **An alternating current field generator that excites a field wire (two or more sensing wires), around which an electrostatic field is created;**

- **An amplifier signal processor that detects changes in the signal amplitude of the sensing wires.**

The alternating current on the field wire creates an electrostatic field in the air between the field wire to ground. When an intruder enters the "field", large amounts of the electric charge flow through the intruder due to the disruption of the field by the human body.

To reduce false alarms, the signal goes through a filter which rejects high frequencies caused by wind vibration and low frequencies caused by objects striking the fence wires. However, the filter allows frequencies associated with intrusion characteristics to be evaluated by the processor. Three concurrent conditions must be met to signal an alarm:

- **The signal amplitude must exceed a preset value that discriminates small animals;**
- **The frequency must be in a range that is associated with humans;**
- **The signal must persist for a set period of time.**

E-field wire configurations are mounted on free-standing posts or chain link fences. All the wires are placed in parallel with each other and to the ground. This will achieve uniform sensitivity along the fence length. Springs are used at the connectors to ensure tension- reducing vibrations caused by wind.

An advantage that an E-field sensor has in comparison with other fence sensors is the self- adjusting circuitry that is built into the processor. Such systems will reject wind and ambient noise. In order to perform, this circuit requires the amplitude of an intrusion attempt to exceed a preset level for a preset period of time.

E-field sensors have a very low nuisance and false alarm rate. Sometimes, countermeasures such as bridging and tunneling can be detected. This depends upon the proximity of the disturbance activity to the sensor. This system should be considered if bridging or tunneling are anticipated intrusion tactics. Other fence sensors (vibration, taut wire) can be added to provide a higher level of detection probability.

Unreliable detection and operation can result:

- From adverse weather conditions (such as rain and snow);
  - Improper installation that results in incorrect tension or insulation coupling;
  - During an electrical storm;
  - Vegetation, grass, or shrubbery movement or growth along the fence line;
  - Animal movement along the fence line;
  - Large spacing between wires (this condition should be avoided because it can allow someone to move between the wires without causing an alarm);
  - EMI can be a problem where multiple systems are deployed in a limited area, unless different frequencies are utilized by each system;
- Any action that causes fence vibration (weather, animals, birds)

#### 40\_3.4.1.1 Defeat of E-Field Systems

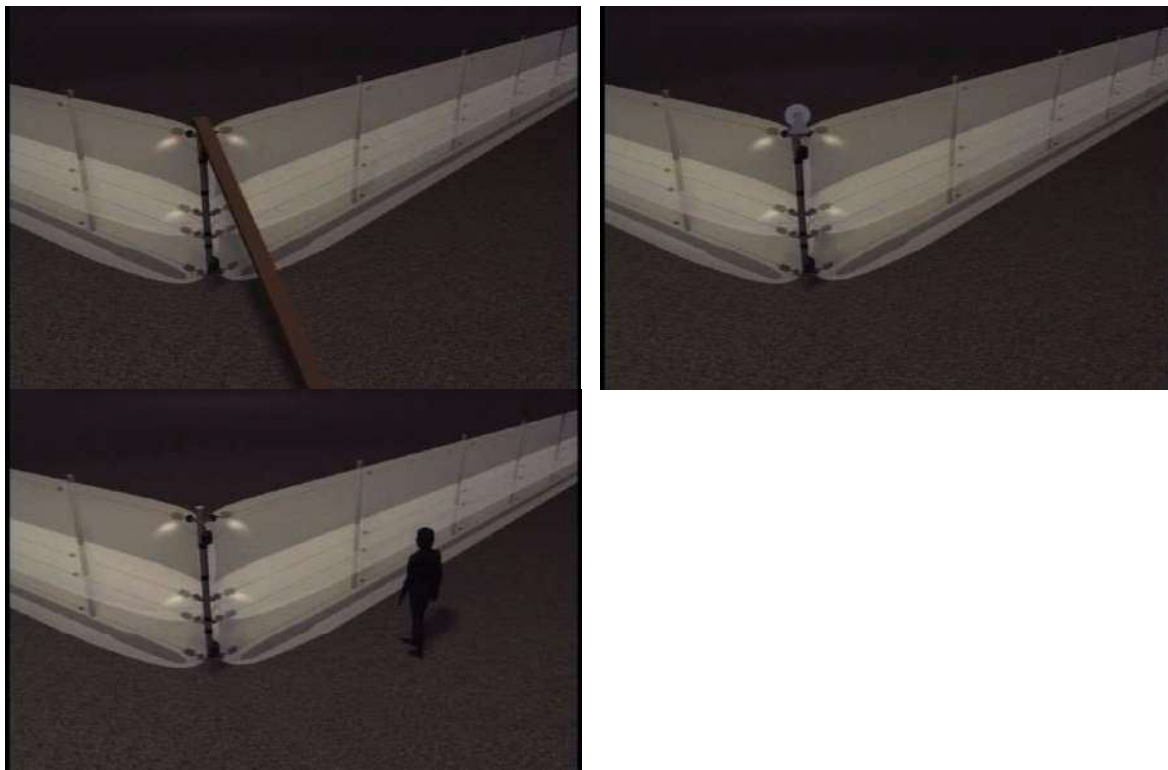


Figure LSS+4057 E-Field systems can be defeated by taking advantage of shadowed areas. Shown is a piece of lumber that can be used to scale the fence at a vulnerable point. Note in the middle photograph a pizza cutter can prevent this practice. An individual in shadow coverage (right) is not

detected. Courtesy of DOE Office of Security and Safety Performance Assurance.

E-Field Sensors can be defeated by:

- Tunneling (six feet or deeper) under the protected area;
- Avoidance by attacking a lack of sensor coverage at buildings and other obstructions. Look for gaps in coverage;
- Bridging, two-man or pole vaulting over the detection zone;
- Alarm stacking.

## ELECTRIC FIELD DETECTION CONFIGURATION/PATTERNS

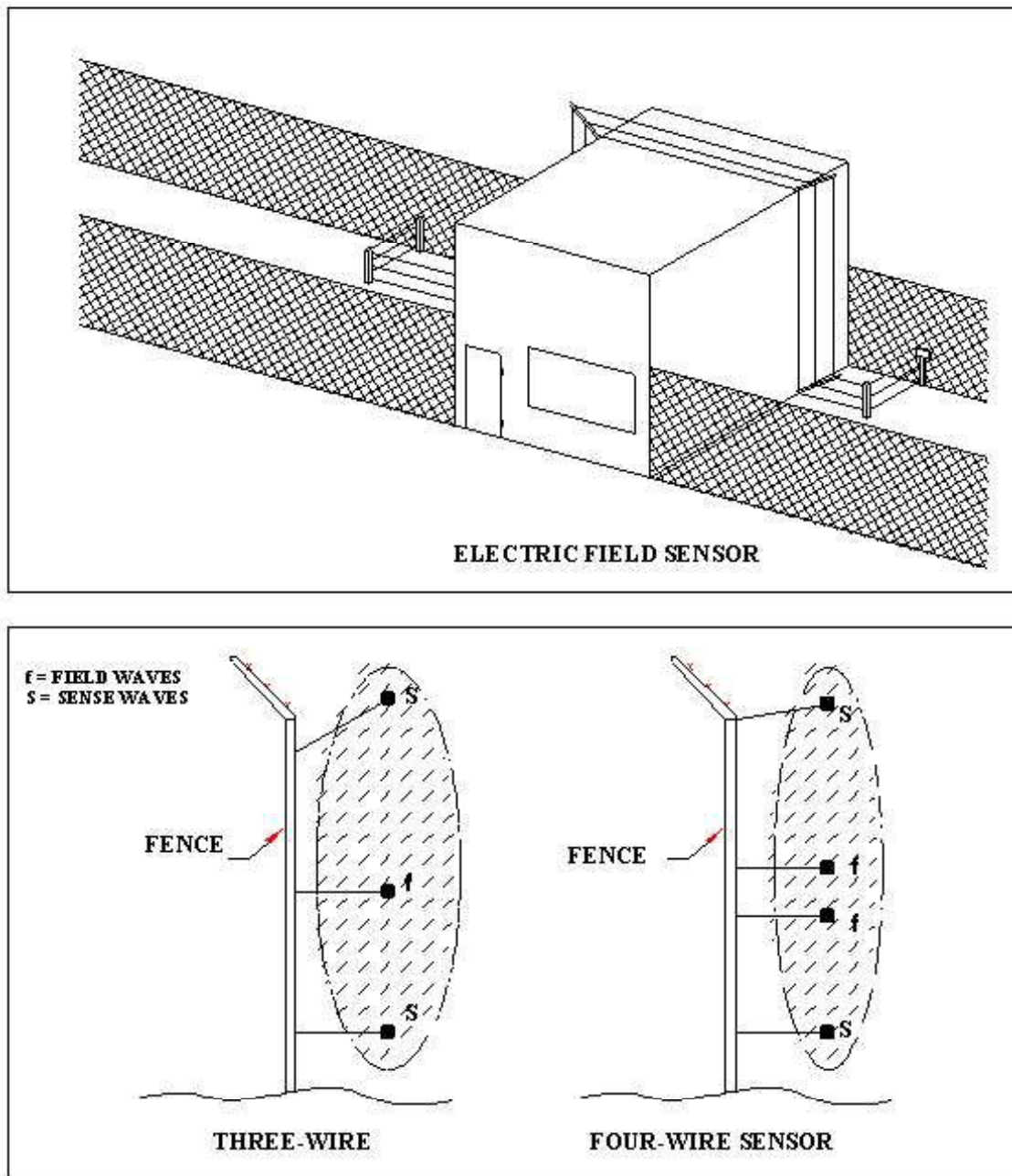


Figure LSS+4021 Electric field detection configuration/patterns

## 40\_3.5 Volumetric Sensors





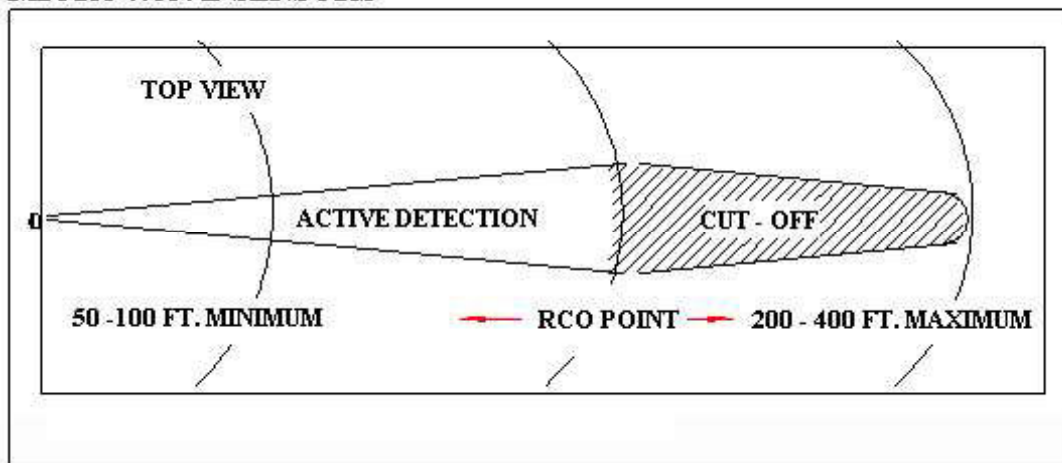
#### **LSS403: DOE on sensor technology**

Volumetric sensors are primarily used for monitoring an intrusion into enclosed areas where entry is through walls, floors, or ceiling. They utilize air pressure, ultrasonic sound, and radio frequency energy as a transmission medium to permeate an entire area and provide information as to changes resulting from penetration.

Volumetric systems are extremely economical where large areas are to be monitored. Because the sensors do not respond until an intruder is within a protected area, they should be installed as part of a comprehensive system of trips. Many different kinds of sensors are available that are reliable, sophisticated, and inexpensive. Often, two different technologies are combined within one detector in order to minimize the potential for false alarms. The most common example is the motion detector that contains microwave and passive infrared.

Volumetric monitoring does not rely upon the physical breaking of circuits that is required when using magnetic trips, foil, or photoelectric devices. The sensors can provide surveillance completely throughout an area from floor to ceiling and wall to wall, rather than just a specific door or window. This is a major advantage.

#### **TYPICAL LONG RANGE DETECTION PATTERN FORMONOSTATIC MICROWAVE SENSORS**



**Figure LSS+4003 Typical long range detection pattern for monostatic microwave**  
2495 22/09/2007 11:42:49 AM  
(c) 1999-2004 Marc Weber Tobias

sensors

**TYPICAL SHORT RANGE MONOSTATIC MICROWAVE  
DETECTION PATTERN**

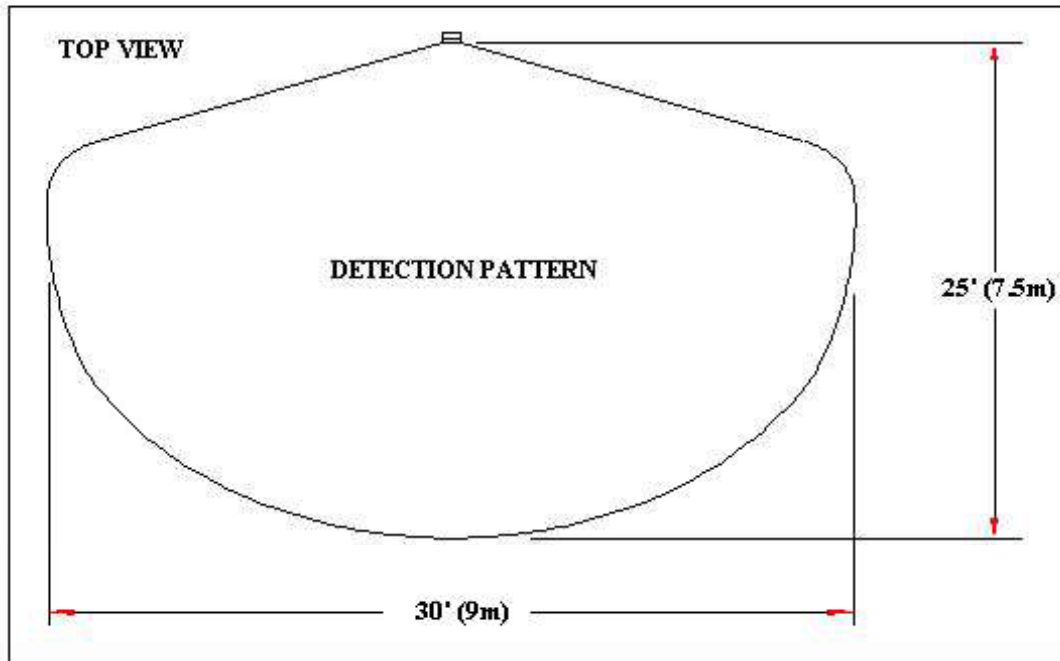
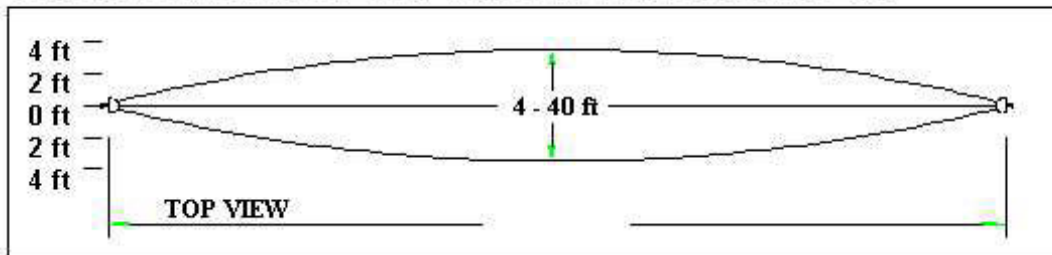
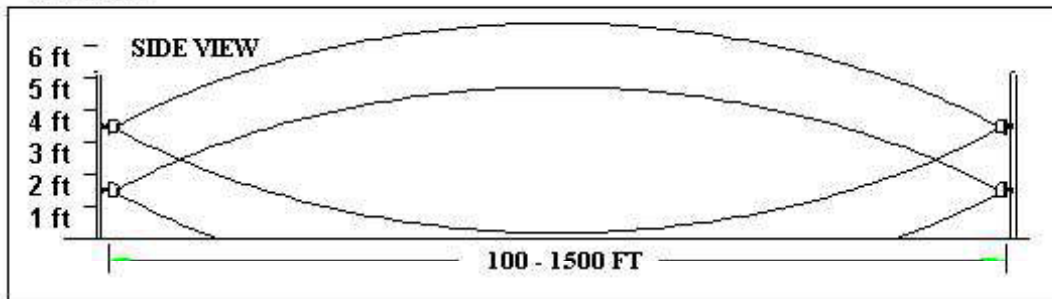


Figure LSS+4004 Typical short range monostatic microwave detection pattern

### TYPICAL BISTATIC MICROWAVE DETECTION PATTERN



\* LENGTH AND WIDTH OF DETECTION PATTERNS WILL VARY, DEPENDING UPON DESIGN.



\* THE MICROWAVE SENSORS CAN BE MOUNTED IN A DUAL CONFIGURATION TO PROVIDE A GREATER PROBABILITY OF DETECTION.

LSS+4005 Typical bistatic microwave detection pattern

## MICROWAVE SENSOR ZONES

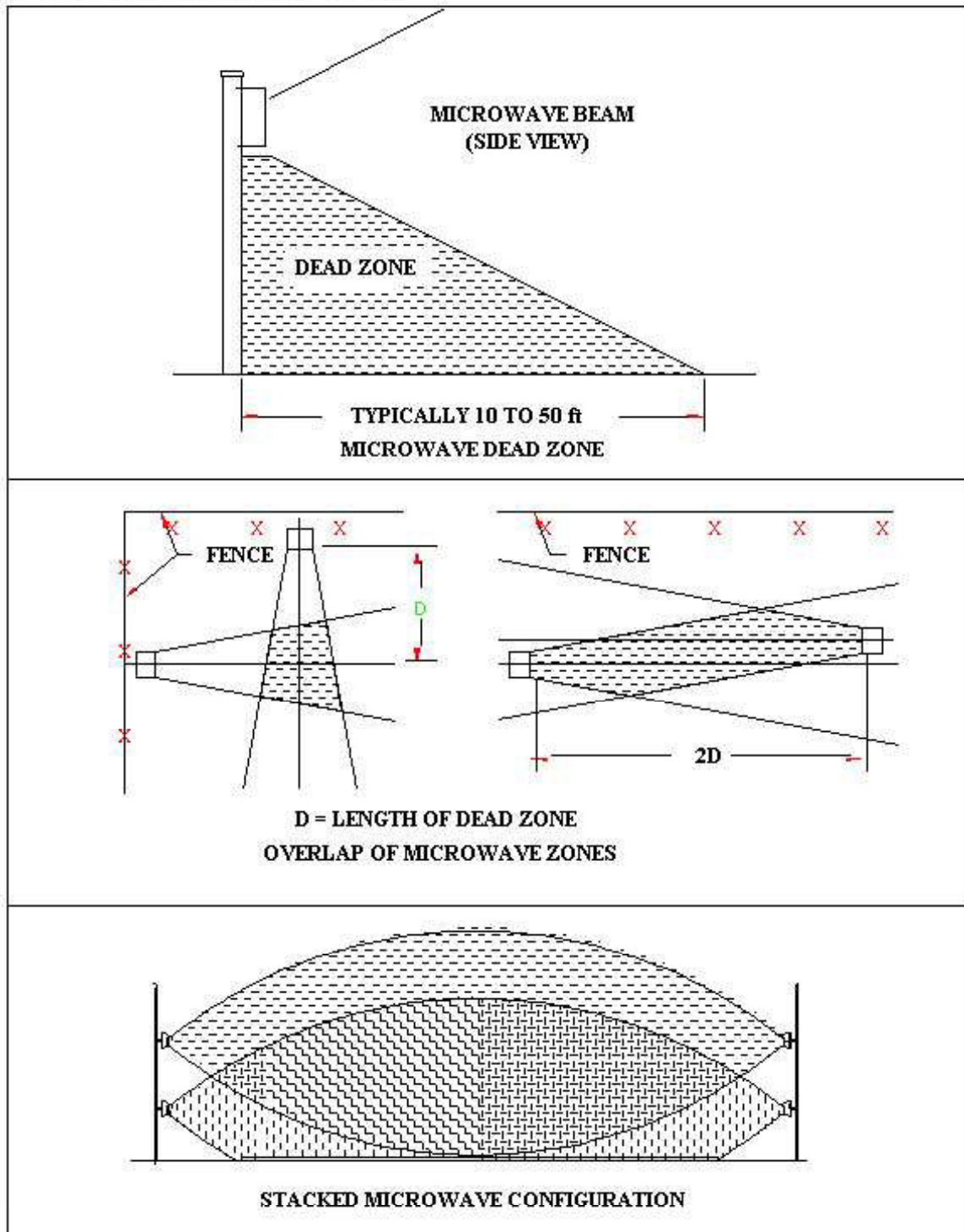


Figure LSS+4006 Microwave sensor zones

### BISTATIC MICROWAVE LAYOUT CONFIGURATIONS

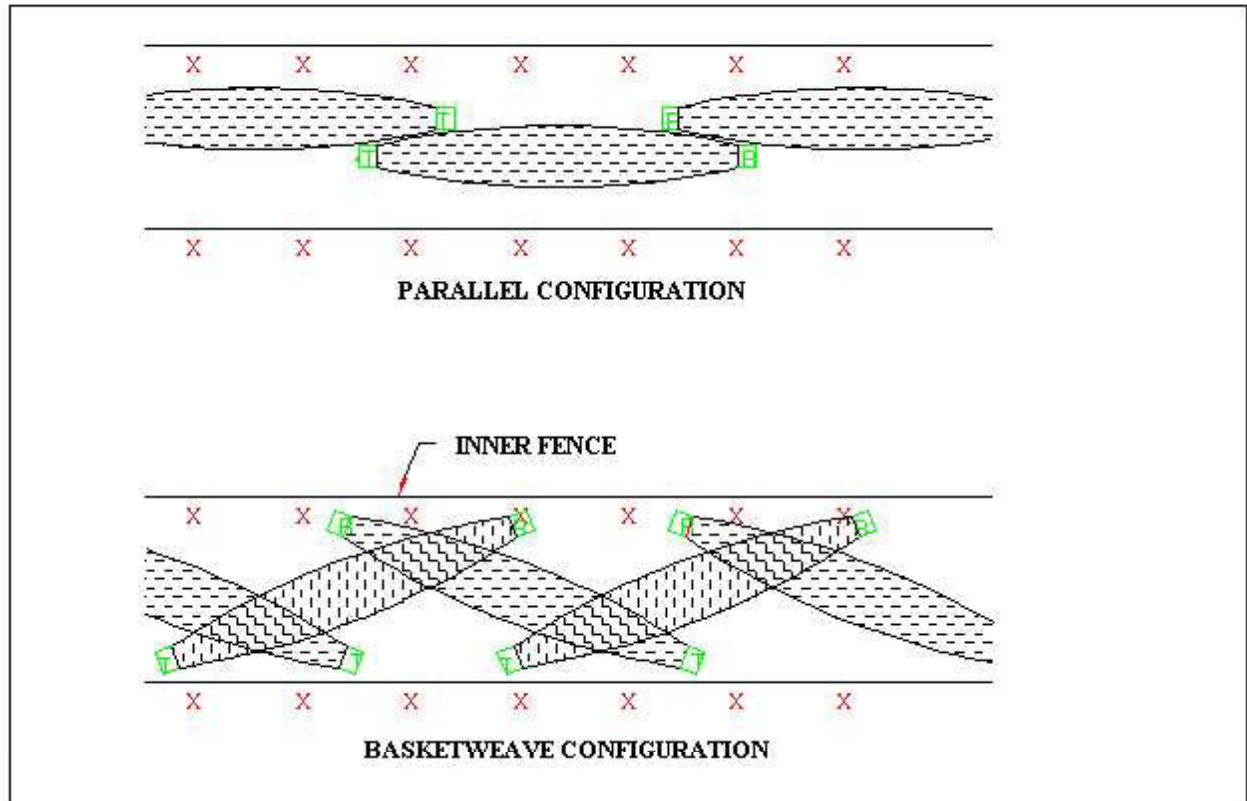


Figure LSS+4007 Bistatic Microwave Layout configurations



### BISTATIC MICROWAVE SENSOR

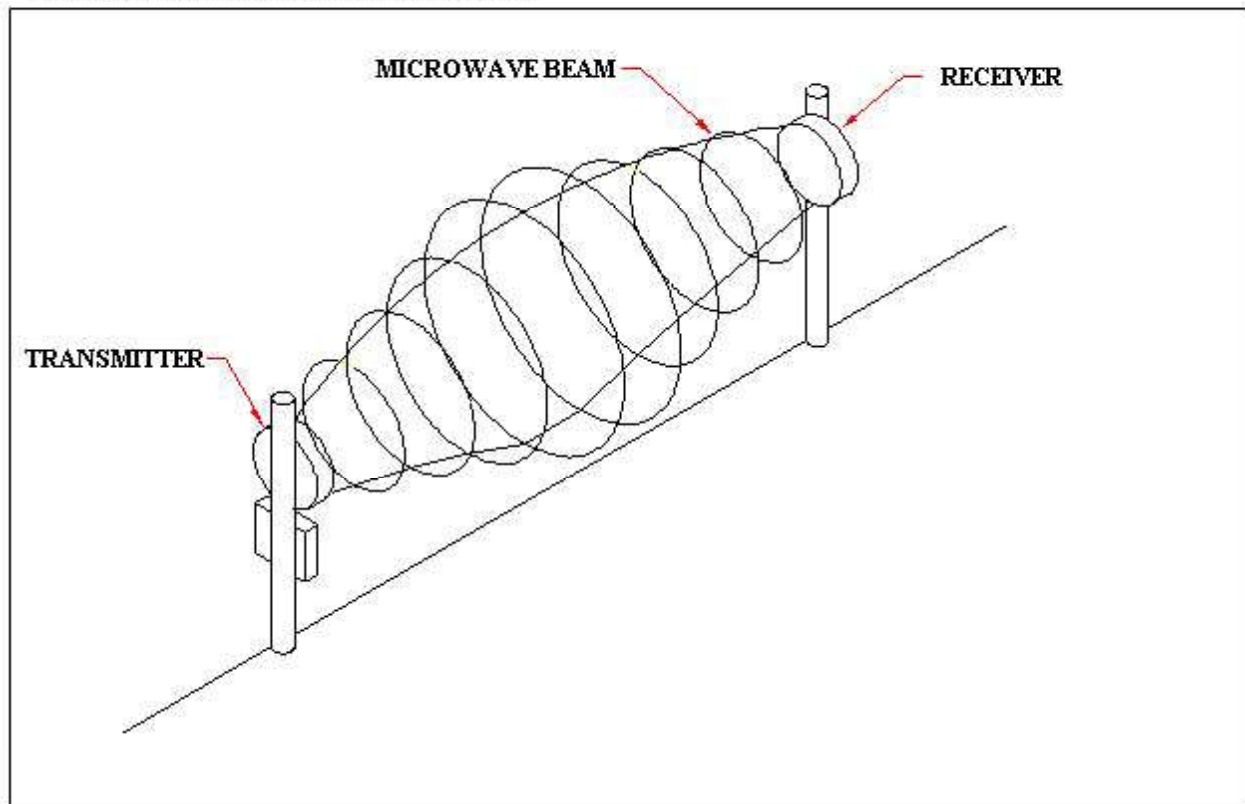


Figure LSS+4008 Bistatic microwave sensor

## 40\_3.5.1 Microwave Systems



**LSS401: Microwave sensor systems**



**LSS402: Issues with microwave sensors**

Sensor technology based upon the transmission of microwaves utilizes radio frequency energy above 10 GHz to protect an enclosed space. The RF will penetrate everything within the target area as well as adjacent barriers. Minute changes in transmitted and received frequencies are compared by a microprocessor for a specific threshold. When the limit is exceeded, an alarm is initiated.

Microwave sensors are motion detection devices that transmit an RF field throughout a protected area. These systems can be utilized for both internal and external applications.

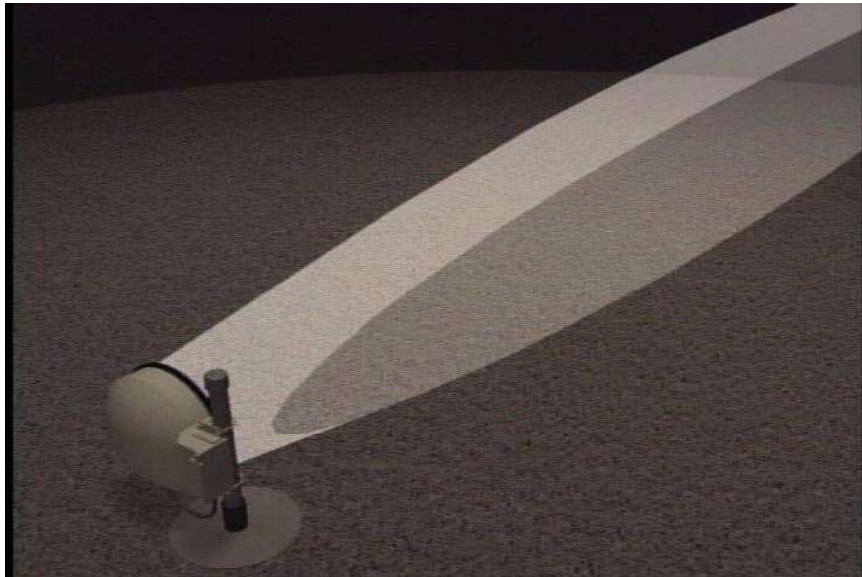
2500 22/09/2007 11:42:50 AM

(c) 1999-2004 Marc Weber Tobias

Microwave devices utilize Gunn diodes to emit low power energy in the "X" band up to 400 feet (line of sight). Microwave devices rely upon the Doppler frequency shift principle that measures a frequency shift between 20 Hz and 120 Hz. These frequencies are generated upon human movement within a protected area.

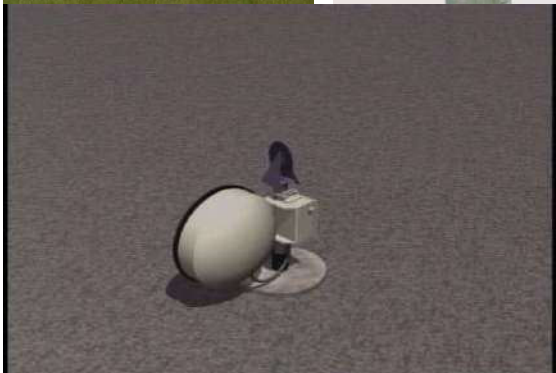
There are two basic types of microwave sensors: **monostatic**, which have their transmitter and receiver encased within a single housing unit, and **bistatic**, wherein the transmitter and receiver are separated, and create a detection zone between them. There are significant differences between the two systems, detailed below.

#### 40\_3.5.1.A Monostatic Units





**Figure LSS+4059** A monostatic system radiates a coverage pattern much like a flashlight beam. The dark gray area shows diminished coverage. Courtesy of DOE Office of Security and Safety Performance Assurance.



**Figure LSS+4049** A microwave system must be protected against a bypass technique of climbing over the sensor.

**A pizza cutter is one method to prevent this practice. The mounting pole should be cut just above the sensor.**

In this configuration, the transmitter and receiver elements are packaged within a single dual function unit. The antenna is mounted within the microwave cavity, and its radiation pattern can be shaped to cover a specific area or detection zone. The actual shape of the beam can be changed to transmit a long, slender beam or a short oval one.

Monostatic systems operate at two distinct frequencies which are rapidly alternated. As each transmitted frequency is turned on or off, the receiver is shut down for a short interval after each transmission. Microwaves propagate at a constant speed; thus the receiver can be specifically programmed to receive those reflected signals that are sent and received from the receiver cut off (RCO) area within a specific time period. This system design allows the user to protect a well defined area and create a "zone of coverage."

#### **40\_3.5.1.B Bistatic Units**



**Figure LSS+4050 Bistatic microwave system**

This configuration requires that the transmitter and receiver be separate units, physically located at opposite sides of the protected zone. The antenna can be configured to alter the signal field (width, height), thereby creating different detection zones. A bistatic system can cover a larger area and would typically be used if more than one sensor is required.

#### **40\_3.5.1.C Placement of Sensors**

Microwave sensors can be used for monitoring exterior areas as well as interior confined spaces such as vaults, special storage areas, hallways and service passageways.

#### **40\_3.5.C.1 Exterior Sensors**

Exterior sensors are utilized to protect an area or a definitive perimeter line, as well as to serve as an early warning alert of intruders approaching a door or wall. Where a well-defined area of coverage is required, monostatic sensors should be used, keeping in mind a coverage limitation of 400 feet. Bistatic sensors can extend their range up to 1,500 feet. Supplementary coverage is recommended for these systems.

Microwave sensors can suffer from false alarms as a result of several factors.

- **Close proximity to other high frequency signals can adversely affect the detection reliability of these sensors because of their operation in the x-band;**
- **Those areas that contain strong emitters of electric fields (radio transmitters) or magnetic fields (large electric motors or generators) can effect the ability of microwave sensors to function properly and should be avoided or compensated for by distinct signal separation;**
- **It is easy to determine the presence of these sensors with commonly available radar detectors;**
- **Bistatic systems are somewhat limited by poorly defined detection patterns. Nuisance alarms may be a problem if large metal objects are nearby or if windy conditions exist;**
- **Zones that contain fluorescent lights can cause unreliable operation, because the ionization cycle created by fluorescent bulbs can be interpreted as motion;**
- **Self generated signal reflection is a common problem. This is caused by improper placement or mounting by positioning the**

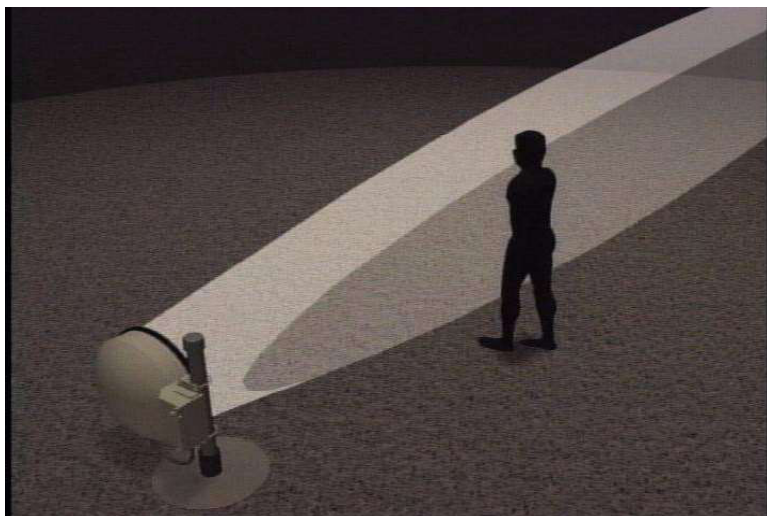
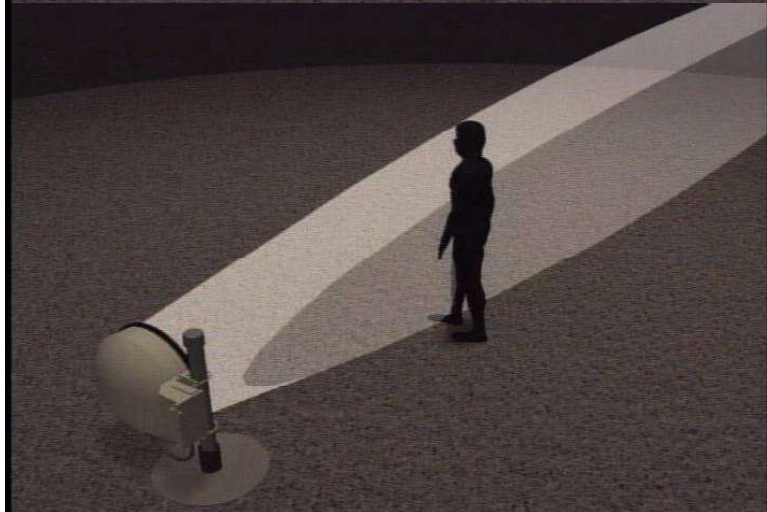
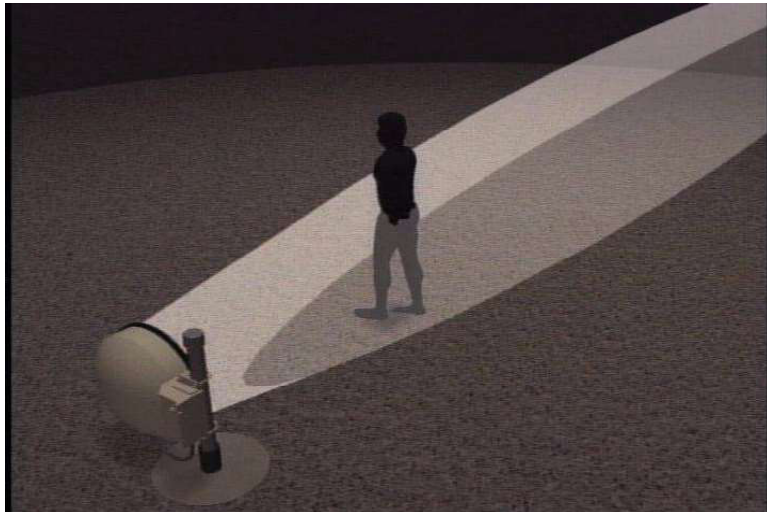


sensor externally and parallel to a wall. The solution is to embed the device within the wall;

- Large metal objects can reflect signals and provide "dead pockets". Such objects should be kept out of the detection zone;
- Microwave transmission will penetrate and pass through walls, glass, sheet rock and wood. Thus, equipment whose operation involves external movement or rotating functions outside or adjacent to a protected zone can cause a false alarm;
- Detectors are not affected by moving air and changes in temperature or humidity, due to the high operating frequency;
- It is essential to test for, note, and compensate for any dead spots (areas of no detection) created by metal objects such as dumpsters, shipping crates, trash cans, and electrical boxes;
- Dead spots and reflected zones can be created by metal objects such as dumpsters, shipping crates, trash cans, and electrical boxes. A careful analysis of such all zones must be made for the presence of non-protected areas. These locations must be noted and compensated for, because they are perfect areas for intrusions. Reflected zones can extend sensor coverage to unintended areas, thus increasing the potential for false alarms;

Microwave systems can be cased by a knowledgeable individual, and walk-through tests can determine the zones of coverage and conversant dead spots that might allow a bypass of the system. The detectors can also be fooled by extremely slow movement within the radiation pattern. The ability to circumvent these systems is enhanced if there are obstructions, as well as energy absorbing clothing. The placement of sensors must be carefully chosen so as not to allow tampering, disabling, or masking. In many burglary investigations conducted by the author, it was noted that sensors had been covered so as not to protect defined zones.

#### **40\_3.5.1.0    Defeat of Monostatic and Bistatic Microwave Sensors**





Monostatic and bistatic microwave sensors can be defeated through a variety of techniques. These include:

#### **Monostatic Microwave**

- Avoidance of detection zone;
- Careful, slow, and deliberate lateral movement;
- Masking of the target through the use of RADAR absorbing material The technique is utilized to mask and create an intrusion path;
- Alarm stacking;
- Avoidance by exploiting poor sensor coverage;

#### **Bi-Static Microwave**

- Tunneling under detection beam pattern;
- Use of a pole or two-man vaulting over detection beam pattern;
- Bridging;
- Stilt walking;
- Slow parallel crawl;
- Slow walk around improper offsets;
- Avoidance;
- Use of noise or RADAR absorption material to create path through detection beam pattern at a very slow movement pace;
- Avoidance by exploiting poor installation coverage, washouts, depressions and snowfall;
- Alarm Stacking.

#### **40\_3.5.1.0.1 Defeat of Microwave Sensors: General Issues**

Microwave sensors can be defeated through many basic techniques, including:

- **Blocking: physically blocking the microwave energy pattern with a containing material;**
- **Very slow and deliberate speed of movement by the intruder, thus avoiding a significant Doppler shift. Remember that microwave is more sensitive to motion that is toward and away from the sensor;**
- **Avoidance;**
- **Use energy absorbing materials;**
- **Use crosswalk motion;**
- **Take advantage of energy blocking, using man made or natural barriers to create a path past the sensor detection pattern;**
- **Bypass the sensor circuit while the system is disarmed**

#### **40\_3.5.1.1 Microwave/Infrared Motion Detector**



**LSS402: Alarm defeat methods for dual technology devices**



**LSS403: Dual technology devices utilized in outside environments**

A Doppler microwave detector is combined (ANDed) with infrared as a dual-mode or dual-tech sensor. The coincidence of alarms from microwave and infrared provides an extremely reliable (lower FAR) indication of intrusion than is obtainable with either sensor alone.

The Dual-Technology sensor utilizes a passive sensor (infrared PIR) and an active sensor (Microwave) that are packaged within one unit. The two detectors are combined in an AND circuit: they both must trigger before there is a valid alarm condition. The areas of coverage for each of the sensors is optimized for overlap.

Dual-tech systems can be deployed along a perimeter line, a fence or a delineated buffer zone, or as a defense against intruders approaching a door or wall. These systems offer both an advantage and limitation in their operation. Although the false alarm rate

is decreased, so also is the probability of detection. This is because two sensors must sense the same condition at the same time. The mathematical probability of detection for the dual-tech unit is the product of the probability of detection for both individual units. For example, if there is a theoretical individual detection rate of 99 percent and 98 percent, the detection percentage for the Dual-Technology (AND logic configuration) drops to 97.02 percent.

There is an inherent problem with dual-technology sensors: passive and active sensors have differing probabilities of detection based upon the movement of an intruder. Remember, the AND gate logic requires coincident signals from both detectors simultaneously to generate a valid alarm. Passive sensors are most effective when an intruder is moving transversely; active detectors work best when the intruder's movement is radial. Thus, the position of the sensor will require a compromise that can diminish detection capability.

So also, any environmental conditions that affect the performance of either sensor will reduce the effectiveness of the system. Notwithstanding these issues, the dual-tech sensors are cost effective and offer greater protection than individual sensors if deployed in a controlled environment.

False and nuisance alarms for the dual technology sensor are infrequent. However, a combination of environmental conditions (e.g. fluorescent lights, heater exhaust) can cause falsing.

Dual-tech sensors can be defeated in certain conditions:

- **Dead spots in the detection pattern (and an intruders knowledge thereof) will permit bypass of all active regions;**
- **Extreme slow movement can be very difficult for microwave sensors to detect;**
- **Blocking or masking of the infrared sensor's field of view can decrease its sensitivity and reduce the probability of sufficient "heat" being detected by, or focused upon the PIR portion of the sensor. Silicone spray or Vaseline can be used to defeat the sensor unless anti-masking software is operational;**
- **Walking into the PIR sensor, rather than across its field of view can reduce the detection capability of the sensor by not**



**"breaking" the boundaries of the PIR detection beams.**



This photograph shows a dual-technology microwave/passive infrared sensor that was defeated in a major diamond theft in Antwerp, Belgium. Silicone was used to mask the device and prevent its proper operation.

#### **40\_3.5.1.2 RADAR**

Radar (RADio Detection And Ranging) is an active sensor that was introduced in the early 1940s. Since its first deployment as a mode of detection, the technology has been vastly enhanced and improved. These sensors operate in the ultra high frequency region of 100 MHz. to 1 GHz. Transmitted signals are bounced off of objects within zones of protection. A processor will evaluate the signal to determine relative size, azimuth and distance. RADAR and microwave systems are quite similar in concept and design, although their operating parameters are quite different. These systems are quite useful, for example, for the detection of planes or helicopter-borne intrusions that would bypass ground-oriented sensors and microwave systems.

As with the previously described microwave systems, there are two basic types of radar sensors: monostatic and bistatic. However, their operation is different than traditional microwave.

With monostatic sensors, detection of intrusion is achieved by the radar transceiver rotating in a preset "sweep" pattern. During rotation, the transceiver emits high frequency energy pulses, forming and scanning a detection zone. When a moving, foreign, or new object is detected, a Doppler shift in the reflected energy is created. When the magnitude of the reflected energy surpasses the preset criteria stored within the processor, an alarm is generated.

The transmitter in a bistatic configuration is typically creating a designated "sweep" pattern, with receivers at several locations that are designed to maximize the potential for detection. The transmitter generates a field of high frequency energy, which "bounces or reflects" off of "foreign" objects and is sensed by one or more receivers.

Radar sensors are best utilized to monitor exterior areas, although in some situations radar sensors can be used to monitor large interior open areas. Optimum performance requires that the ground be reasonably level and the perimeter boundaries straight. If portions of the perimeter are hilly or have crooked boundaries, the radar unit may be elevated to provide a better line of sight view. Radar sensors can also be used to monitor the straight and level sections of the perimeter, while other types of detectors (e.g. in-ground sensors or video motion detection) can evaluate the remaining sections.

Safe havens for intruders can be provided by "Dead zones" that are created by large objects, buildings or hill masses or depressions. Extreme weather conditions such as rain or snow storms can decrease detection potential of radar. False or nuisance alarms can be caused by the detection of foreign objects not within defined zones resulting from the undesired reflection of RF energy.

Uneven terrain can create "hidden pockets." So also, a slow and low approach by an intruder may defeat sensors.

## 40\_3.5.2 Ultrasonic Systems



### LSS402: Ultrasonic alarm sensors

Ultrasonic sensors operate above a frequency of 19 KHz and function similarly to microwave in many respects. They are based upon the Doppler theory and sense minute changes in forward and reflected waves caused by absorption characteristics of the intruder. Whereas microwave systems utilize super high frequency (SHF) radio waves, the ultrasonic device will transmit sound waves above the normal hearing range.

### 40\_3.5.2.1 Passive Ultrasonic

The passive Ultrasonic sensor "listens" for ultrasonic sound energy that has a frequency range between 20-30 KHz in a

protected area. The frequencies in this range are generally associated with intrusion attempts representative of metal striking metal, hissing of an acetylene torch, and shattering of concrete or brick. The sounds thus generated are transmitted through the surrounding air and travel in a wave-type motion. The detector evaluates the patterns against stored characteristics.

Ultrasonic sensors are typically mounted on a wall or ceiling and are frequently used in tandem with another sensor, such as a passive device (Passive Infrared-PIR) to provide a greater probability of detection (PD). Environmental issues can increase FAR, depending upon the variability and uncontrollability of the characteristics of the zone. These devices are unaffected by heat changes within a protected area. Unlike microwave and radar, ultrasonic energy can be easily contained within a defined area because it does not pass through obstructions such as walls, roofs, or partitions. Unfortunately, waves do not pass through furniture or other obstructions such as boxes and crates and can thereby create dead zones which must be protected by other sensors.

False alarms and unreliable detection can result from a number of conditions:

- **Extreme changes in temperature or humidity from those conditions that existed at the time of installation and calibration;**
- **Any noise within the ultrasonic range;**
- **Air movement from heating and air conditioning systems;**
- **Drafts from doors and windows;**
- **Hissing from pipes;**
- **Dead zones which are created from objects and material that block transmission from sensors;**
- **Anything that causes movement, such as animals;**
- **The ringing of a telephone.**

Passive ultrasonic sensors have a limited frequency spectrum; sounds caused by an intrusion that fall outside the unit's spectrum (such as drilling), may not generate an alarm.

### PASSIVE ULTRASONIC MOTION SENSOR

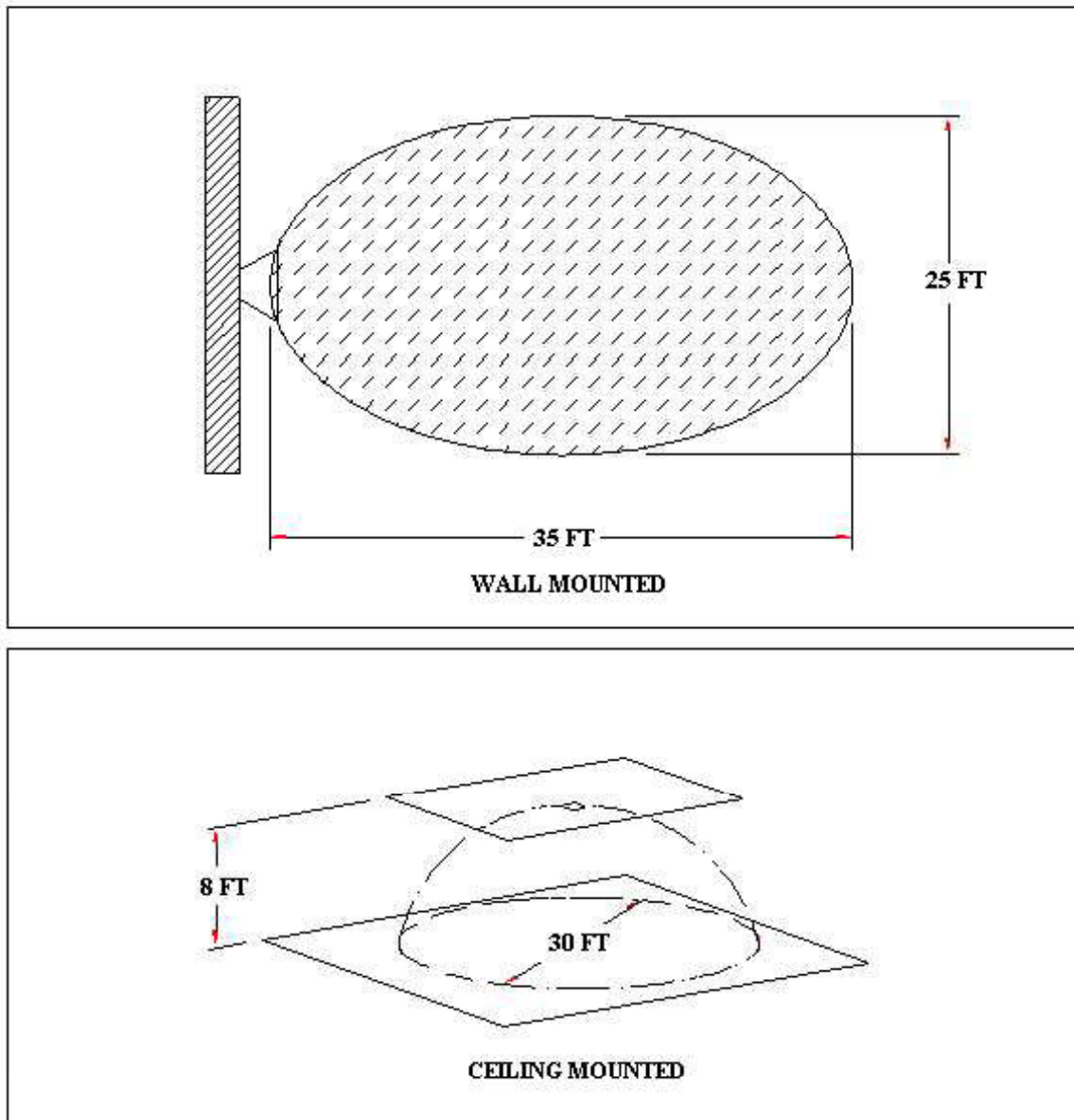


Figure LSS+4011 Passive ultrasonic motion sensor

### 40\_3.5.2.2 Active Ultrasonic

The active ultrasonic sensor emits sound energy into a defined area and reacts to a change in the reflected energy pattern. These sensors operate on a theory based upon a frequency shift in reflected energy. Ultrasonic sound is transmitted from the device

in the form of energy through the air in a wave-type motion. Waves are reflected back to the receiver and provides a sound signature of the protected area. Any disturbance will cause the reflection to occur faster, thus changing the frequency slightly. Both passive and active ultrasonic sensors are installed in virtually the same manner.

Unreliable detection can result from many causes. See the listing of conditions in the above section.

Active ultrasonic systems can often be defeated by slow horizontal movement across the area of coverage. Proper calibration is critical to minimize this potential. A knowledgeable and properly equipped intruder can use special "test lights" to detect coverage patterns and circumvent these areas.



### ACTIVE ULTRASONIC MOTION SENSOR

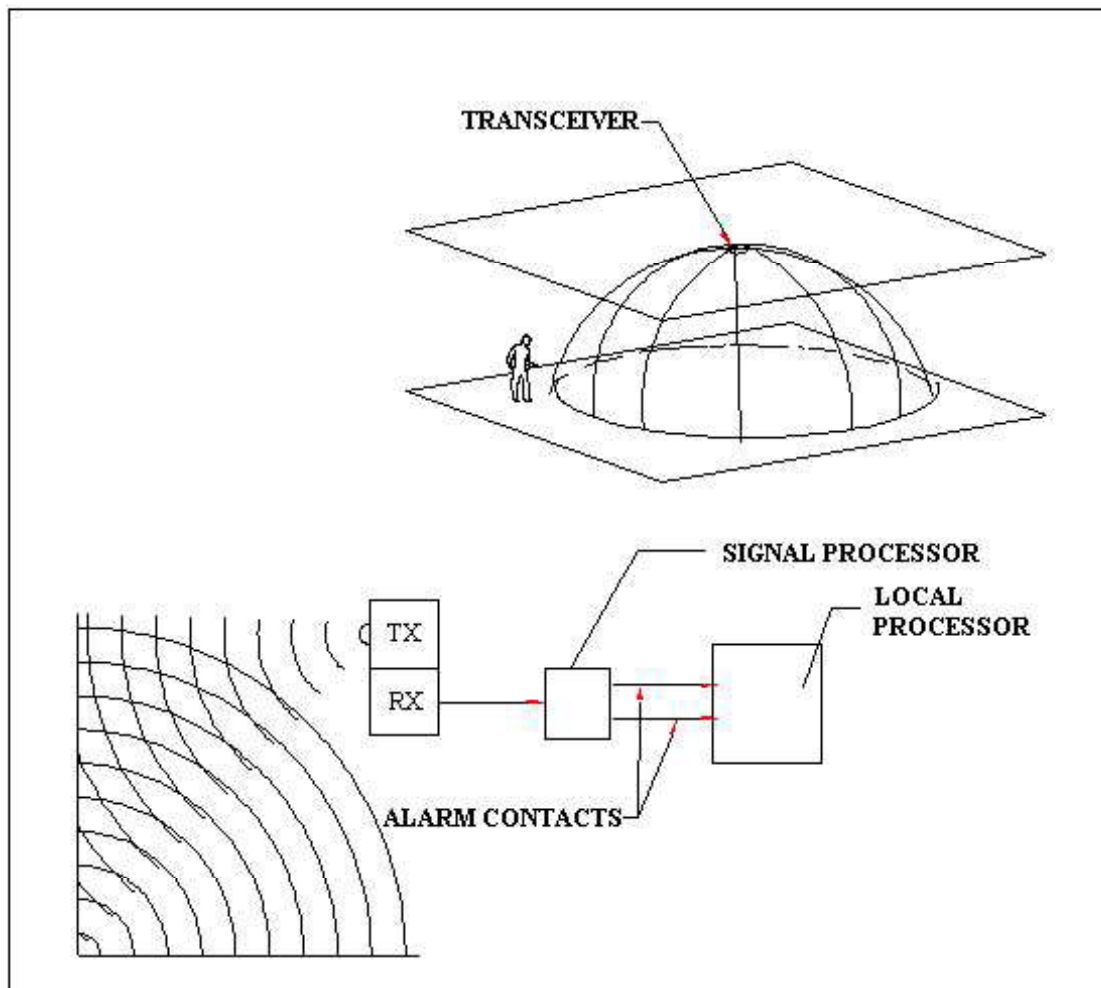


Figure LSS+4012 Active ultrasonic motion sensor

### 40\_3.5.2.3 Audio Sensors

Certain sensors are designed to listen to the audible range for noises that are created by intrusion into protected areas. These detectors are generally utilized within structures rather than being subjected to the outside environment. The system is usually comprised of microphones (transducers) that are mounted on walls or ceilings, and a processor that analyzes noise signatures that are consistent with the protected zones and possible intrusion attempts.

It is essential in the design of these systems that sensors be

located in areas where the predicted intrusion noise will exceed the normal environmental noise floor. Failure to properly calibrate the detectors will result in noise masking, making it impossible to differentiate ambient from intrusion generated sounds. These sensors are generally utilized in conjunction with other systems, such as motion detection or photoelectric, to insure a high probability of detection. Sometimes, audio detection is combined with thermal imaging motion detection. This can provide for a record of both audio and visual tracking of a break-in. Audio sensors are particularly well suited to this application because they are not sensitive to the thermal environment and florescent lighting. If excessive background noise is present, the audio sensor should not be considered.

Erratic or unreliable detection can result from:

- **Improper setup and calibration that affects sensitivity settings either positively or negatively, causing the detector to react to extraneous background noise, such as clocks, office equipment, boilers and heating or air conditioning units;**
- **Excessive background noise, such as airplanes, trains or loud weather conditions (thunderstorms) may cause significant noise levels);**

Slow, deliberate actions by an intruder can defeat these sensors. Likewise, muffling the normal sounds of movement while intentionally allowing sufficient lag time to occur between any noise generated can bypass the detectors.

#### **40\_3.5.2.4 Acoustic Detection (Air Turbulence Sensors)**

Acoustic air turbulence sensors detect low frequencies (within a range of 20 - 40 Hz, depending on the model) created by helicopters that are in their final landing phase or at close range (one to two miles), and are utilized for intrusion attempts. Some of the quietest helicopters, such as the Hughes 500C, Bell 47, Bell 206, and the Jet Ranger, have been detected at distances up to 500 feet. For increased probability and reliability of detection, detector sensitivity is typically set for a range of 300 feet.

Typically, such detectors are employed because traditional systems, such as perimeter and in-ground technology would be bypassed. These devices "listen" for basic sound pressure

generated by helicopter rotor blades and engine. There are four specific signatures that are sought:

- **Downward wash, caused by the energy that is required by the rotor blades to maintain airborne status;**
- **Blade slap, which originates from the forward traveling blade as it penetrates the trailing tip vertex remaining from the previous blade passage;**
- **Tail rotor, which is directly geared to the main rotor that generates harmonically-related frequencies;**
- **Engine noise, which is not usually muffled because of the power needed for rapid changes in flight performance.**

In order to assure reliable detection of inbound aircraft, regardless of their approach once they enter the protected zone, such areas should be covered by overlapping sensors. With proper design, there is no restriction on the distance of sensors from the main control unit; thus, zones of protection can extend for miles.

Unreliable detection and false alarms can result from the following causes:

- **Location of sensors near to any vehicular or road traffic, especially truck movement;**
- **Location of sensors near railroad right of ways;**
- **Location of sensors near anything that generates pressure or wind turbulence. Sensors are particularly sensitive to broadband noise;**
- **Turbulence generated at a distance and conveyed by air pressure propagation;**
- **Pressure caused by wind viscosity and the roughness of the terrain;**
- **Sensitivity settings set too low to compensate for vehicular traffic;**
- **Improper spacing of the sensors, allowing some areas not to be covered by the detection pattern.**

These systems will not detect airborne assaults that utilize other flying technology, such as glider, parachute, or ultra light.

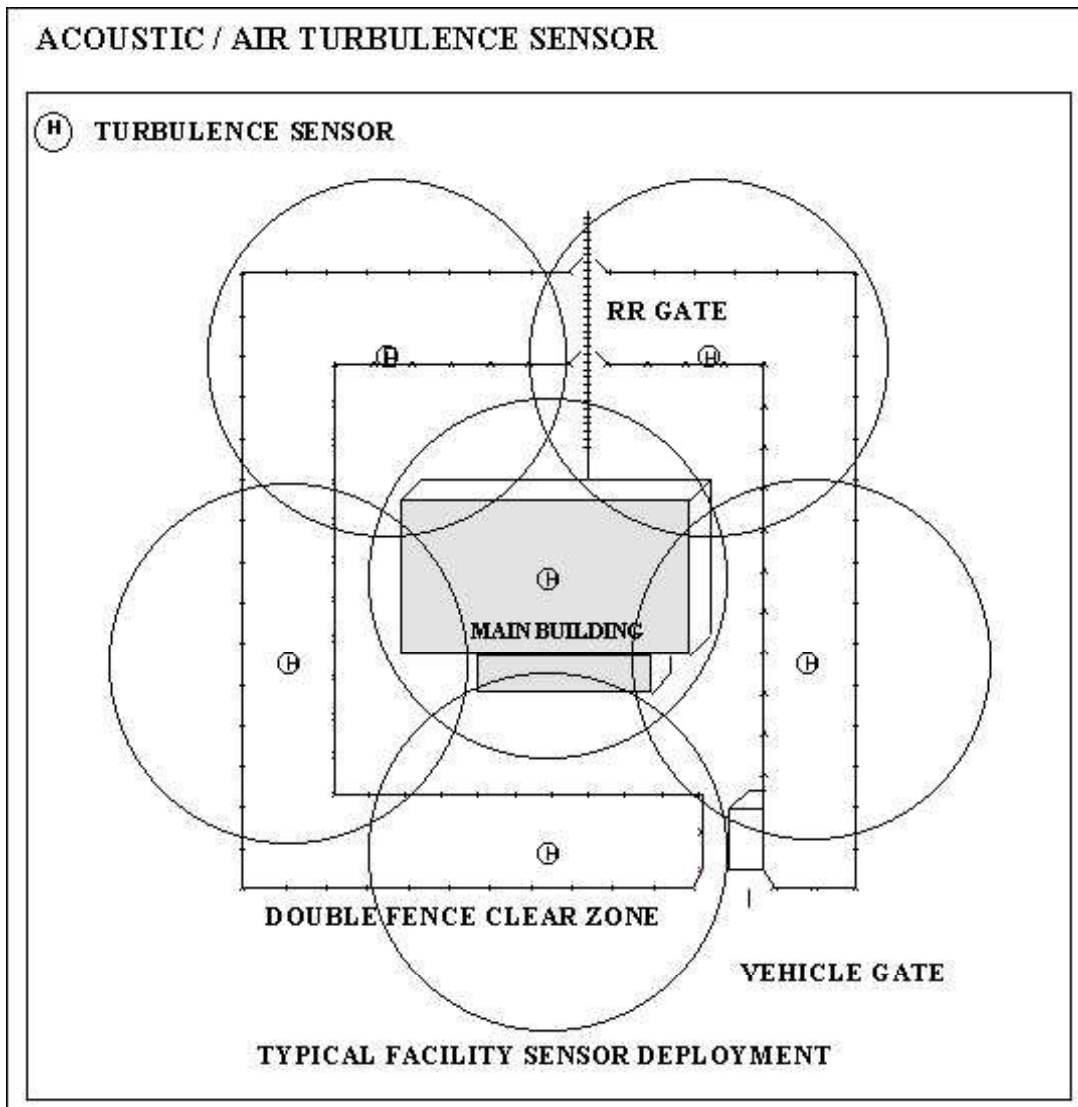


Figure LSS+4034 Acoustic/air turbulence sensor

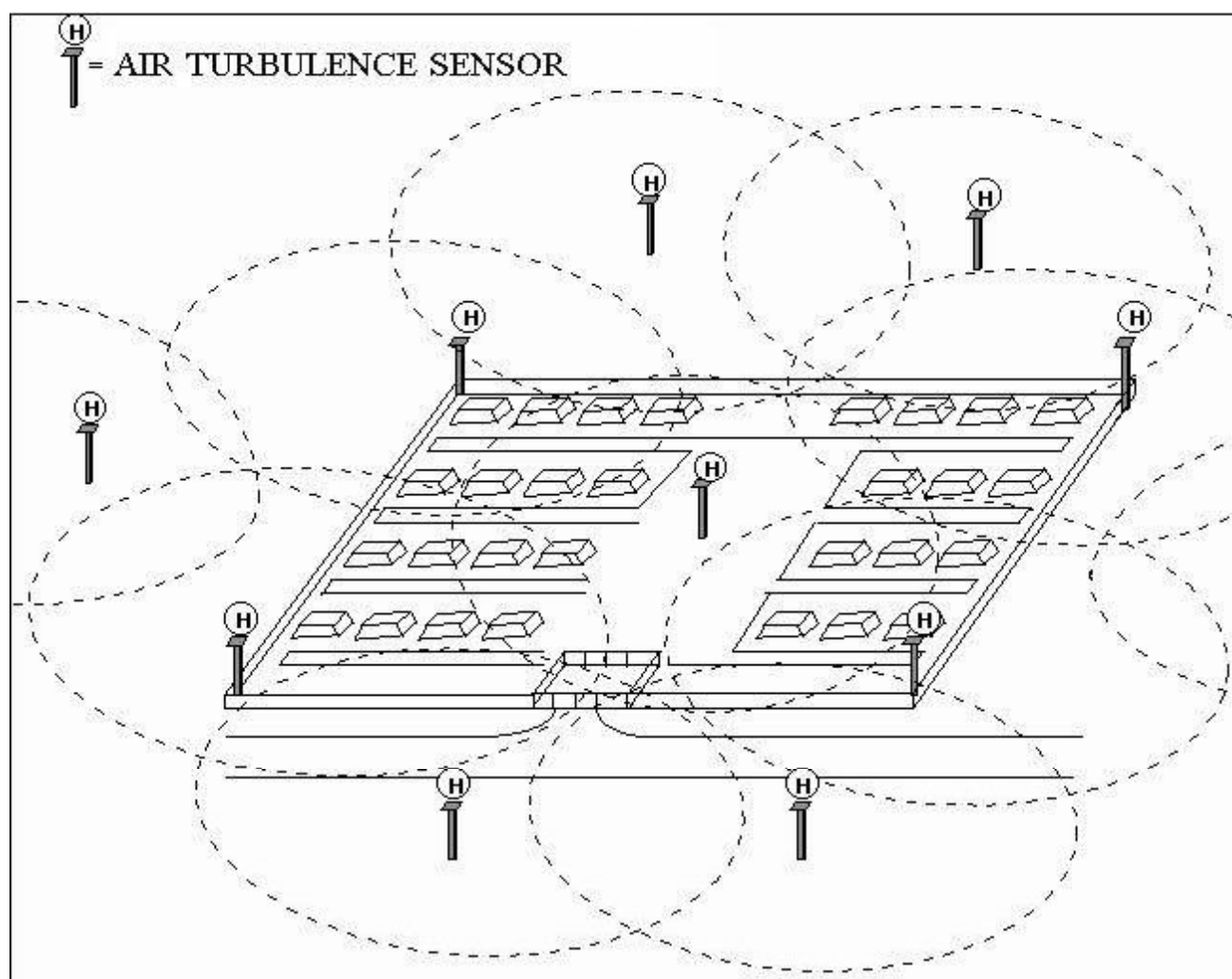


Figure LSS+4035 Logistic/munitions storage complex

#### 40\_3.5.2.5 Defeat Techniques for Infrasonic and Ultrasonic Sensors

Sensors that utilize sound, either below or above the normal range of hearing, are subject to defeat by employing a variety of techniques. These are summarized for all forms of sound energy sensors. It should be noted that these systems, which operate between 20-45 KHz. may bother pets, due to their increased sensitivity to sounds above the normal range of human hearing. This may provide an indication that ultrasonic energy is present.

#### Infrasonic

2519 22/09/2007 11:42:54 AM  
(c) 1999-2004 Marc Weber Tobias

- Entry through opening that does not create infrasonic waves, such as a sliding door or window;
- Concealment within protected area;
- Masking detector;

**Active Ultrasonic** This type of sensor is more sensitive to motion toward and away from sensor.

- Very slow intrusion speed and movement, thereby avoiding a significant Doppler shift;
- Use of ultrasonic energy-absorbing blanket or material, including aerosol Styrofoam filler;
- Blocking the transceiver or using an object to block the transmitter;
- Spoofing the sensor into believing it is secure. Use Freon gas, water or similar substances;
- Create a loud noise to create a false alarm;
- Use of a high power transmitter at the same frequency;
- Use crosswalk motion;
- Take advantage of man made or natural barriers that create a path past the sensor detection pattern;
- Bypass the sensor circuit while the system is disarmed;

#### **Passive Ultrasonic**

- These sensors have a limited frequency spectrum of sensitivity. Exploit the fact that certain intrusion sounds outside of the sensitivity of the sensor (such as drilling) will not activate it;
- Alarm stacking;
- Bypass the sensor circuit while the system is disarmed;

#### **Active Sonic**

- Use of very slow movement by intruder;
- Use of energy-absorption blanket or other material;
- Block the transceiver by using tape or other material;
- Take advantage of natural barriers in the protected area to avoid detection;
- Spoofing;
- Alarm stacking;



- Bypass the sensor circuit while the system is disarmed.

### 40\_3.5.3 Operational Difficulties with Volumetric Systems

Volumetric sensors are prone to technical operating problems and failures if they are not installed correctly. The following guidelines apply to their use:

- RF fields in microwave systems may penetrate through walls into adjacent facilities, registering movement in areas not intended to be monitored. This can cause a false alarm;
- Propagation patterns for microwave systems may not completely cover a desired space. This can be due to irregular shapes of rooms to be protected or a shielding effect of items within the coverage area;
- Frequent false alarms may result if precise testing is not periodically done for a specific area, in order to take into account physical differences;
- Ultrasonic systems will not penetrate adjacent walls, ceilings or floors;
- Ultrasonic sensors will detect heat and can be triggered by hot air turbulence;
- Ultrasonic detectors may register a false alarm from heating and air- conditioning equipment, sonic booms, thunder, jet aircraft, and other shocks;
- Ultrasonic systems, unlike microwave, cannot be set to protect a close pattern or area;
- Microwave is more stable than ultrasonic.

### 40\_3.6 Heat Detection: Passive Infrared Sensors



LSS401: Outside passive infrared sensors



LSS401: Thermal imaging and sensing



LSS402: Passive infrared sensor technology



**Figure LSS+4051 A thermal imaging sensor will detect body heat of an intruder.**

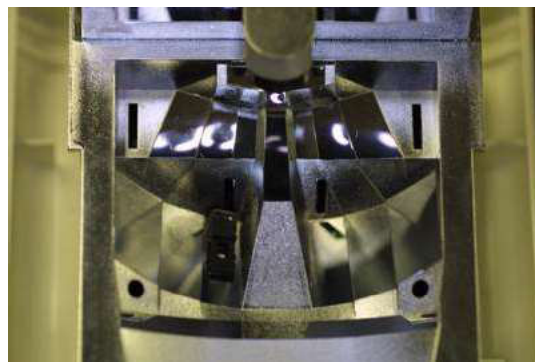
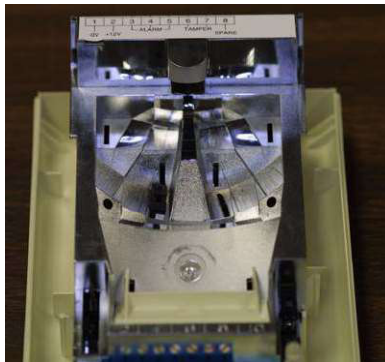
The wavelength of infrared radiation lies between  $.7 - 100 \mu\text{m}$  in the electromagnetic spectrum, and is slightly higher than radio waves. It is not visible to the human eye but is perceived by the heat receptors of the skin. Energy in the form of rays is transmitted or reflected by all objects, even a block of ice. The amount of radiation and its frequency are dependent upon and directly proportional to structure and temperature of the surface. Thus the sun, having a surface temperature of  $6000 \text{ C}$ , radiates IR in the visible spectrum at a wavelength of  $.3-.8 \mu\text{m}$ . In comparison, the human body gives off energy at a frequency of  $7-14 \mu\text{m}$ . In order to avoid capturing environmental thermal deviations, rate of change measurement circuitry or

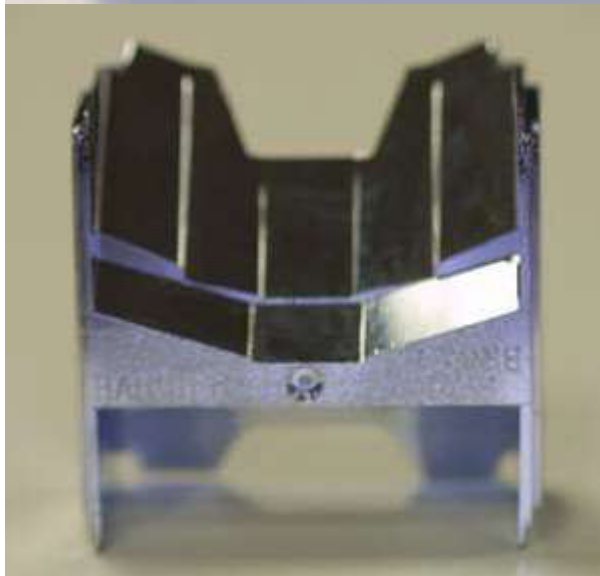
bi-directional pulse counting circuitry is employed.

The PIR wavelength is subdivided into two major range detection categories: one covers **near infrared energy** (e.g. thermal energy emitted by TV remote control devices), and the other covers the **far infrared energy** (e.g. thermal energy emitted by people). It is this latter category which is employed in security applications.

The infrared sensor will detect a narrow frequency band of radiated energy in the target area. It is referred to as a passive device because it receives its information from the area being monitored, but does not transmit any energy. Power consumption is low, in contrast to active devices such as microwave that require emission of RF.

Passive IR devices are constructed with a multi-segment concave mirror and infrared measuring sensor at its focal point. The shape, size, and number of such segments will vary, depending upon the design of the detector and the coverage pattern. Some areas of the mirror will be sensitive to IR; others will not. The sensor head is typically divided into several sectors or zones, each correlated and defined for specific boundaries. Detection occurs when thermal energy is emitted from a heat source and this energy crosses two adjacent sector boundaries or crosses the same boundary twice within a specified time.



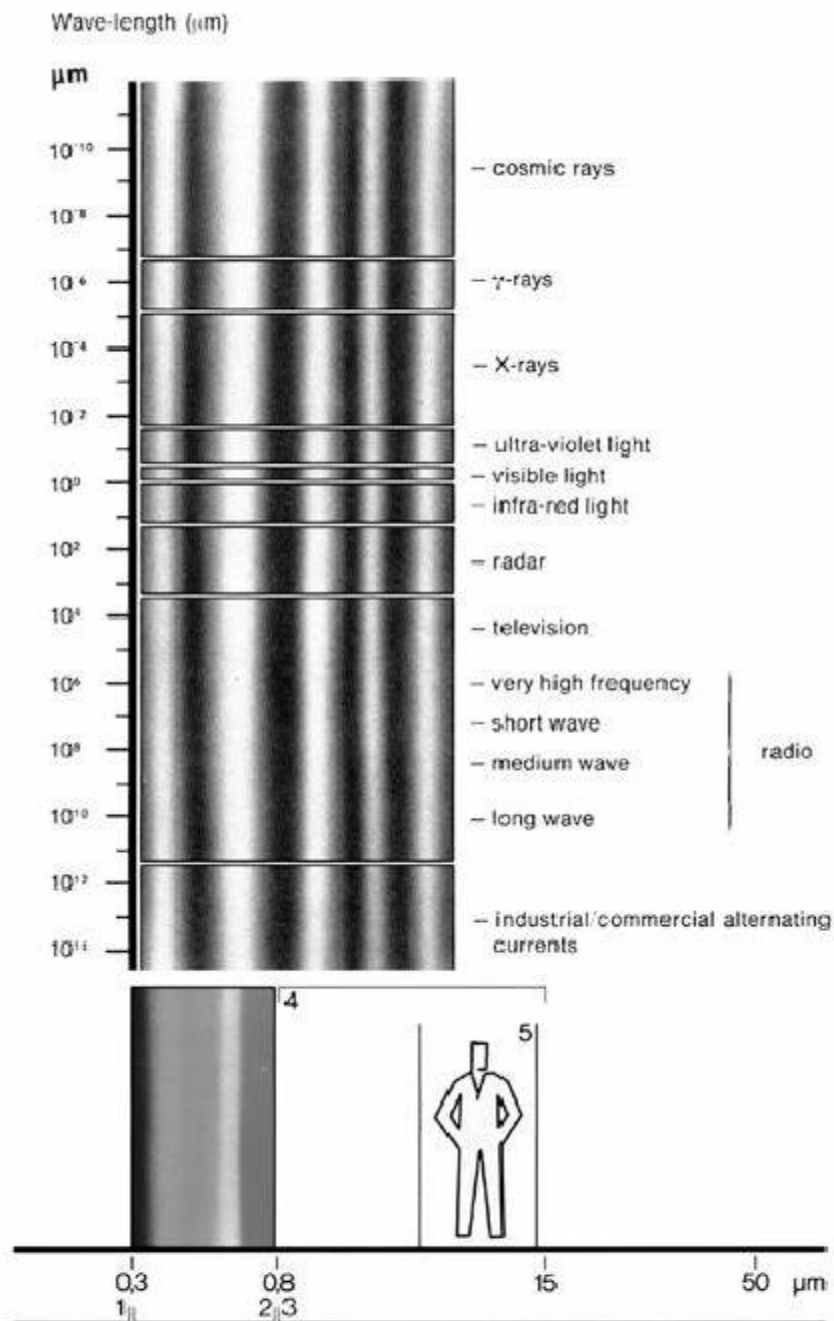


**Figure LSS+4052 A variety of lens configurations are utilized for infrared sensors to**

2524 22/09/2007 11:42:55 AM  
(c) 1999-2004 Marc Weber Tobias

**focus energy on the sensor and create zones of protection.**

The processor will compare the intensity of signals between a moving object and its background, taking into account distance. A threshold value will be set to minimize false alarms. There must be a sudden, rapid, and substantial increase in energy before a valid alarm is triggered. Temperature variations caused by heating, air-conditioning or blowing wind will not be recorded because they do not occur rapidly enough. Passive IR devices operate within a temperature range of -10 C to +50 C.



These sensors detect (but do not measure) electromagnetic radiated energy generated by sources that produce temperatures below that of visible light. They are sensitive to the change of thermal radiation. PIRs "see" or "detect" infrared "hot" images by sensing the contrast between the "hot" image and the "cooler" background.



In rate of change measurement, the processor evaluates the speed at which the energy in this field of view changes. Movement by an intruder in the field produces a very fast rate of change, while gradual temperature fluctuations produce a slow rate of change. In the bi-directional pulse counting technique, signals from separate thermal sensors produce opposite polarity. An unprotected or unshielded human that enters a field of view and moving at a typical speed (walk or above) will normally emit or produce several signals which allow detection to occur.

Optics and reflective principles play a very important role in the design and function of PIRs. Because of the need to precisely focus thermal radiation, the reflection and focusing of the energy waves is done in two ways: **reflective focusing** and the **fresnel lens** method.

**Reflective focusing:** The energy waves are reflected off a concave mirror and directed into the sensing element. **Fresnel lens:** This technique allows the energy to travel directly to the sensor. Both methods use some type of protective covering on the sensor, so that the loss of some energy is unavoidable. The performance of both sensors is excellent.

Passive infrared sensors are usually installed on walls or ceilings, aimed at and defining the desired protection zone. Each detection/surveillance zone can be thought of as a "searchlight" with the beam width gradually widening as the zone extends farther from the sensor. Different segments will be illuminated while others are "dark". This design characteristic allows the user to focus the "beam" on areas where protection is needed while ignoring other areas, such as known sources of false alarms. Tower or ceiling-mounted PIRs theoretically provide a 360 degree detection pattern.

A PIR looks for thermal radiation projected and in contrast with a cooler background; its sensitivity is based upon the detection and comparison of temperatures. As the environment approaches the same temperature as the intruder, the detector become less sensitive. This is especially true for environments ranging between 80-100 degrees. Theoretically, if a person was radiating the same temperature as the environment, he would be invisible to the sensor.

There are several reasons for false alarms:

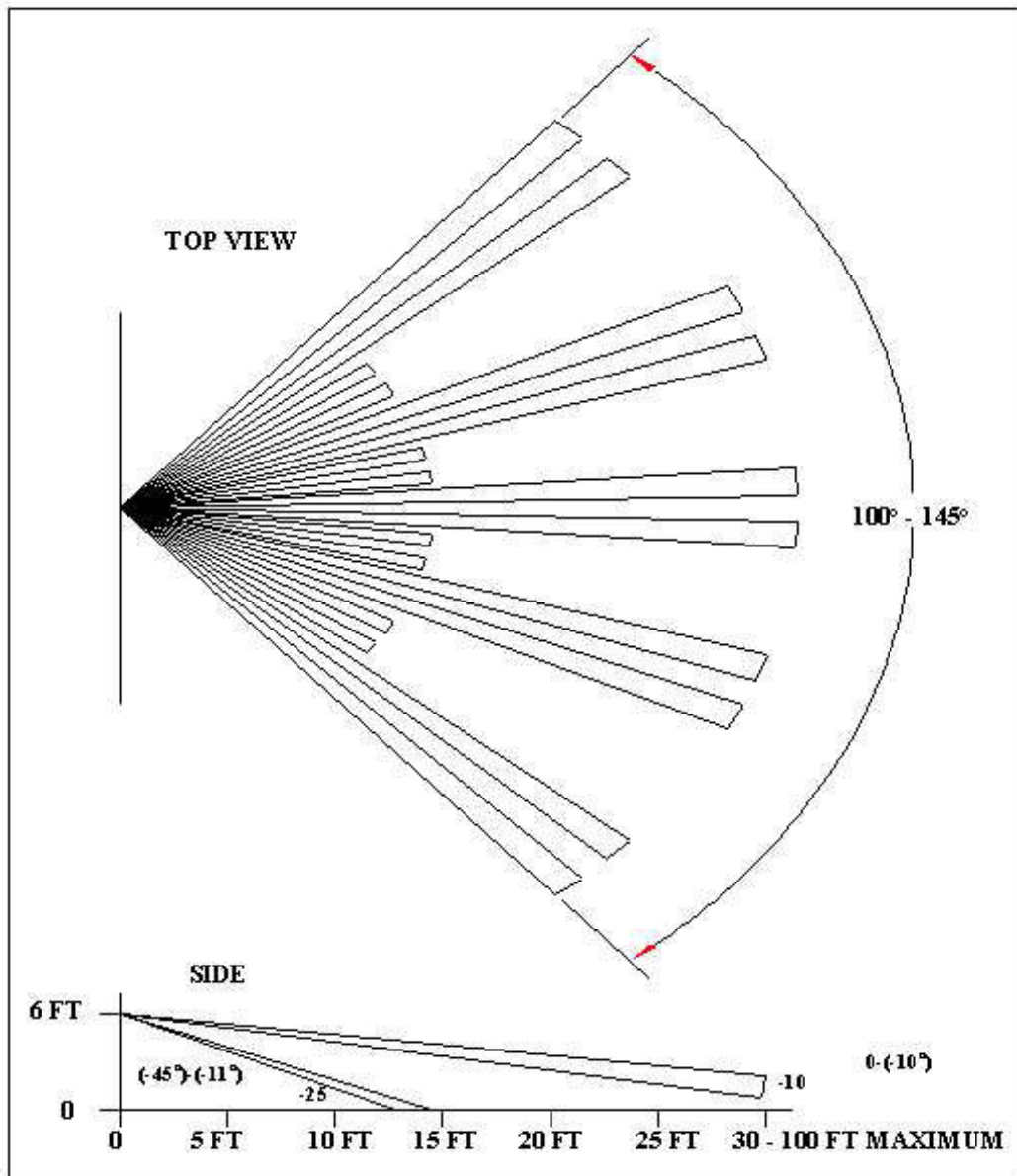
- Heat radiating from small animals or rodents;
- Time-activated space heaters, ovens and hot water pipes within the field of view;
- PIR sensors that are not designed with the capacity to ignore visible light can be affected by car headlights or other sources of focused light;
- Objects in a room can become heated over time and subsequently begin emitting or reflecting infrared energy. This can occur from sunlight. If the light is, in effect, turned on and off, such as by the movement of clouds, an alarm can be generated.



**Figure LSS+4053** An infrared sensor is blocked from proper operation. The sensor is on the far wall in the corner.

Shadowing, cloaking or masking the intruding heat source from the field of view can decrease the probability of detection. This is because it reduces the possibility of sufficient radiated or emitted heat from being focused on the thermal sensor. A knowledge of the dead spots of the detection pattern can permit an intruder to bypass active regions. Walking into the sensor rather than across the sensor's field of view can also reduce the detection capability. In the photograph above, the sensor is located in a warehouse and is blocked by storage of items, greatly reducing its reliability.

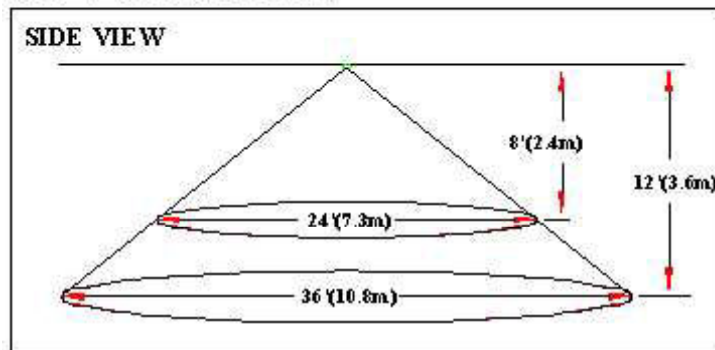
## PASSIVE INFRARED SENSOR



THE NUMBER, RANGE, AND PROJECTION ANGLES OF THE DETECTION BEAMS VARY DEPENDING UPON DESIGN.

Figure LSS+4013 Passive infrared sensor

**TYPICAL PIR COVERAGE PATTERN  
(CEILING MOUNTED)**



**DISC FLOOR BEAM  
PATTERN**

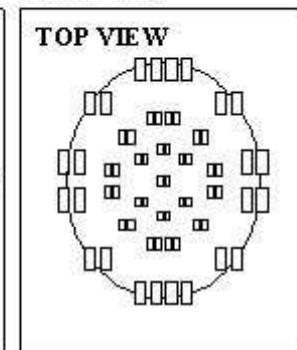


Figure LSS+4014 Typical PIR coverage pattern (ceiling mounted) and disc floor beam pattern

**TYPICAL PIR CURTAIN DETECTION PATTERN (WALL MOUNTED)**

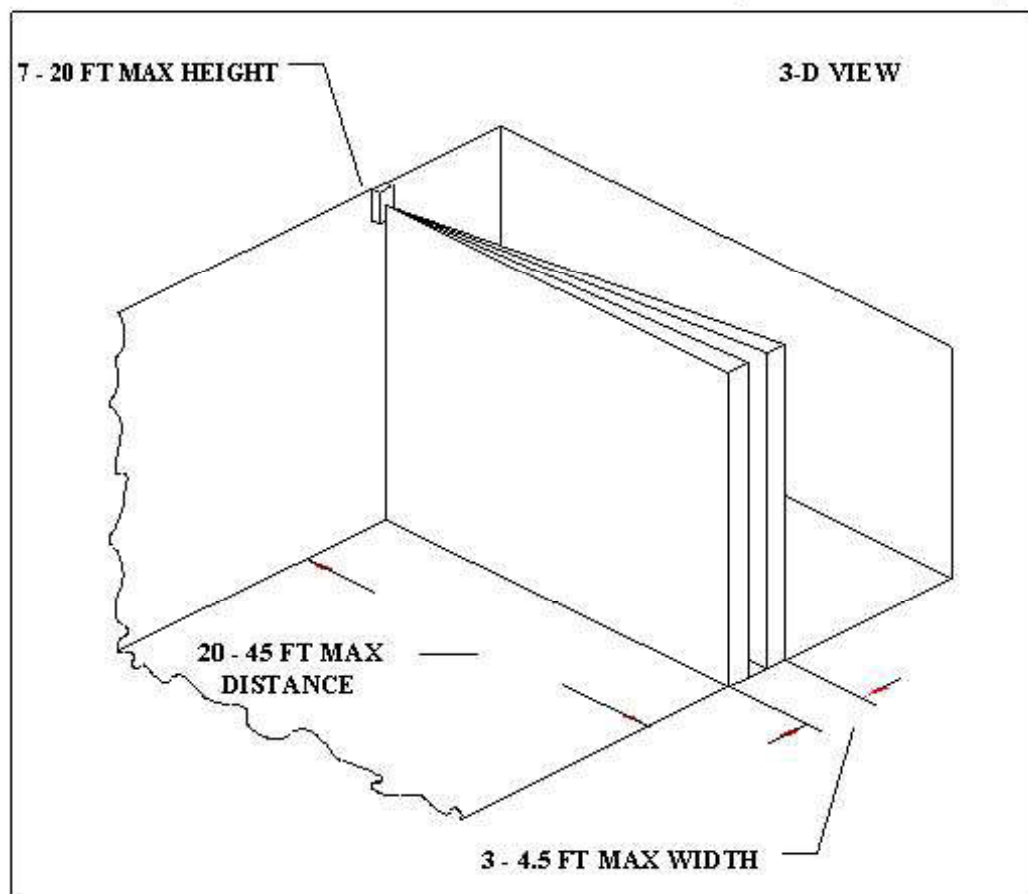


Figure LSS+4015 Typical PIR curtain detection pattern (wall mounted)

## PASSIVE INFRARED

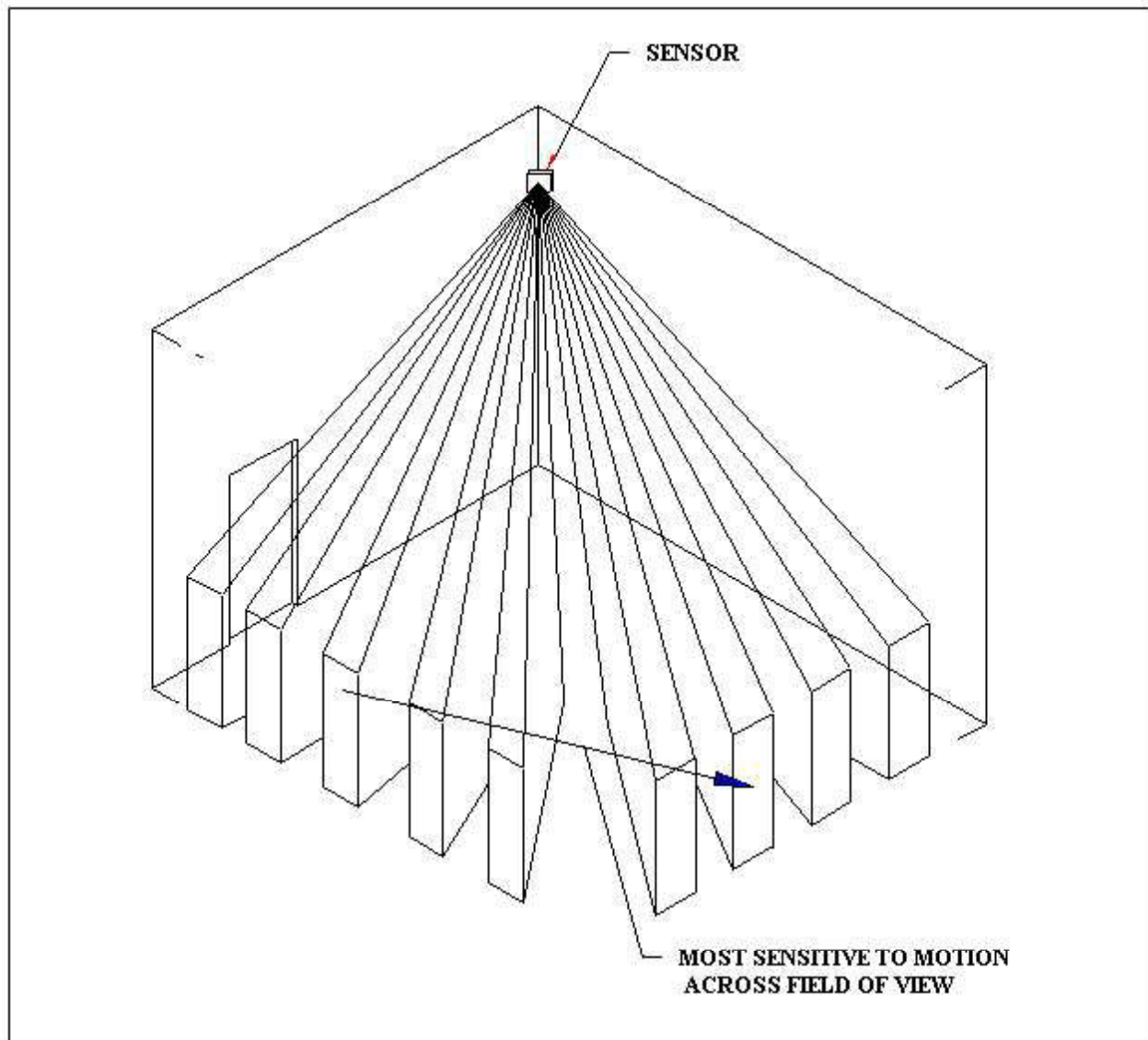


Figure LSS+4016 Passive infrared

### PIR COVERAGE/PLACEMENT PATTERNS

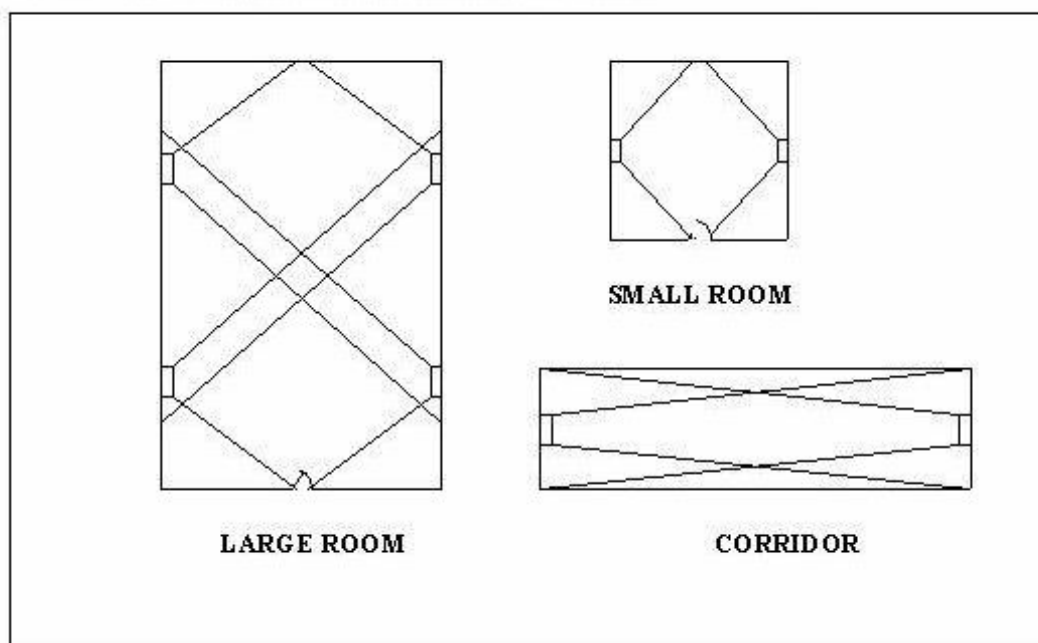


Figure LSS+4017 PIR coverage/placement patterns

## 40\_3.6.A Interior Active Infrared

Interior active infrared sensors transmit a curtain-pattern of modulated infrared energy for a designated area of protection. The sensor reacts to a change in the modulation of the frequency or an interruption in the received energy, both caused by an intruder.

These sensors are comprised of a transmitter and receiver that are packaged within a single unit. A laser is utilized for the source. Its plane is projected onto a special retro-reflective tape that is employed to define the end or edge of the protection zone.

Energy is reflected from the tape, back to the receiver. This energy passes through a collecting lens that focuses the rays onto a cell which then converts the IR to an electrical signal. The processor evaluates the signal level: if it drops below a specified threshold for a defined period (caused by an intruder), an alarm will be generated.



Depending upon the reflectivity of the tape, coverage patterns can be between 15-25 feet wide by 17-30 feet long. The laser plane angle can be adjusted from 37° to 180°. The temperature of the environment nor the speed or direction of the intruder have any affect on detection characteristics. Thus, the systems are quite reliable.

There are a number of conditions that can cause unreliable operations or false alarms:

- Dust or other particles collecting on the surface of the reflective tape;
- Any degradation of the detection capabilities of the sensor;
- Reflective tape must have no gaps and be continuous;
- The angle from the sensor to the ends or corners of the tape must not exceed 45 degrees;
- The activation of an incandescent light which shines directly into the sensor;
- Incandescent lights greater than 100 Watts (or sunlight) falling directly in line with the tape will be reflected back to the receiver with a sufficient magnitude to trigger an alarm;

Interior active infrared systems can be defeated by the avoidance of the projected laser plane by a knowledgeable intruder. He can determine the location of the field of the potential detection pattern from the placement of reflective tape; he can then plan his movements to avoid detection.

### ACTIVE INFRARED MOTION SENSOR

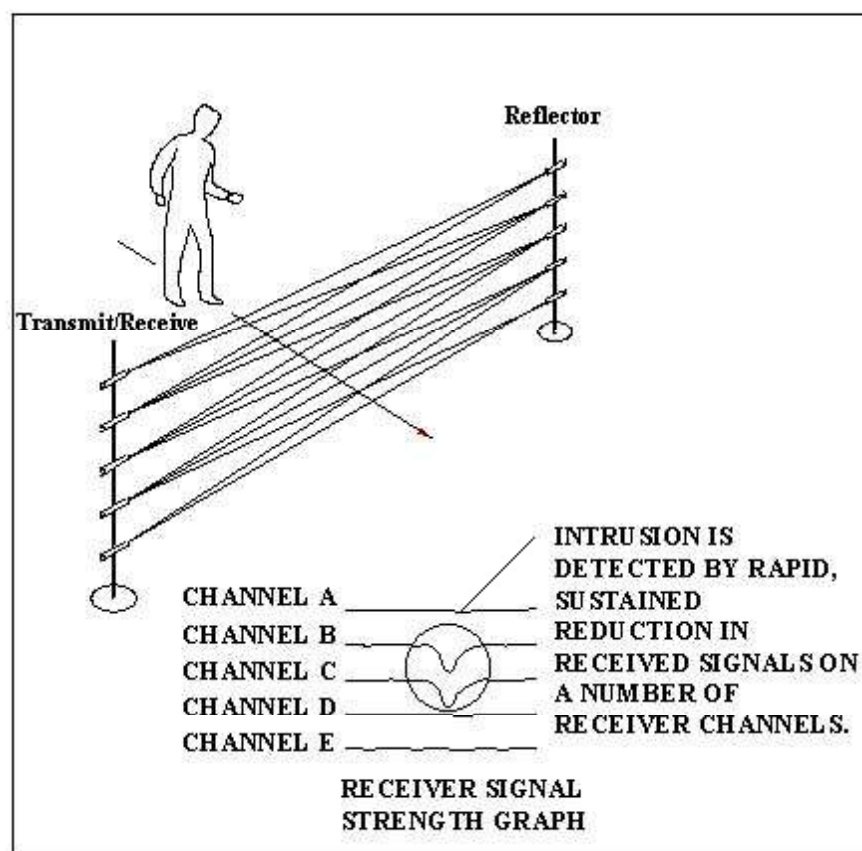


Figure LSS+4018 Active infrared motion sensor (Interior)

## 40\_3.6.B Exterior Active Infrared

In the active infrared design, the transmitter and receiver are separated by the protected zone. A modulated multiple frequency straight-line beam is generated, producing an electronic fence, much like the photoelectric beam system. An interruption in the received energy or the modulating frequency can trigger an alarm.

These sensors are line-of-sight devices, and therefore require that the area between the two units must be uniformly level and clear of all obstacles and obstructions. Holes can be created in coverage by low spots in the terrains that will disrupt the "coverage" pattern. Typically, active infrared systems are employed in conjunction with a single or double fence barrier which defines the perimeter to be covered. A sensor zone length

can extend up to 1,000 feet.

As with all other optical detectors that utilize separate transmitter and receivers, precise alignment of the emitter-receiver path is critical for reliable detection. The beam width is relatively narrow and requires regular calibration and realignment on a frequent basis. Misalignment can be caused by a number of issues:

- **Movements in the ground (e.g., earth tremors);**
- **Objects hitting the unit (e.g., falling rocks, vehicles, falling trees);**
- **Freezing and thawing of the ground;**
- **Dirt and dust build-up on the receiver or transmitter;**
- **Inadvertent movement of objects into the transmission path;**
- **Extremely heavy snow or rain.**

Reliable operation and detection can be insured in the following circumstances:

- **Freezing ground or extreme winds: deep foundations for the mounting of transmit and receive sensors to minimize movement;**
- **Sensor hitting or jarring: install protective barriers around the sensors;**
- **Snow and grass around the sensors: remove by hand or blower to prevent damage or misalignment;**
- **Poor weather conditions, such as fog, heavy rain, or severe dust or sand: consider another technology, or decrease detection zone to compensate for energy attenuation;**
- **Interaction of animals in the protected area: provide barriers to entry;**
- **Vegetation: do not let it grow to a size that its movement will interfere with the IR path.**

**Bridging or tunneling** is a common method of defeat. There should be no dips or gullies between transmitter and receiver, or they should be brought to a uniform level. The pedestals or columns that the sensors are mounted on can be utilized to support vaulting over them. Overlapping beams can prevent this practice.

### ACTIVE INFRARED MOTION SENSOR

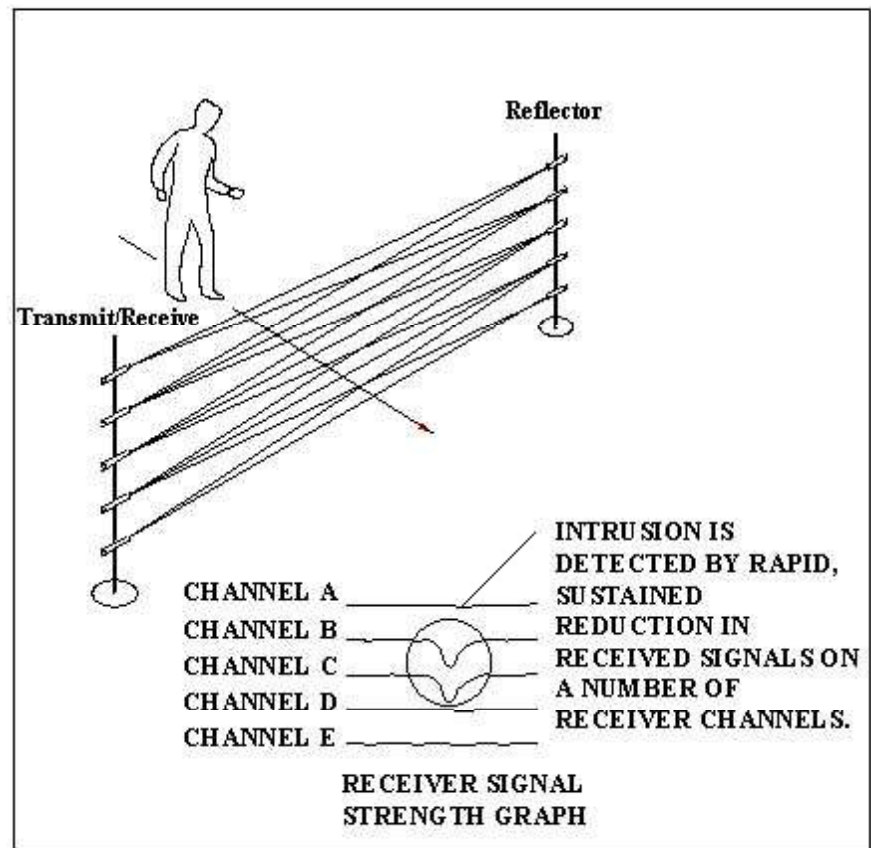
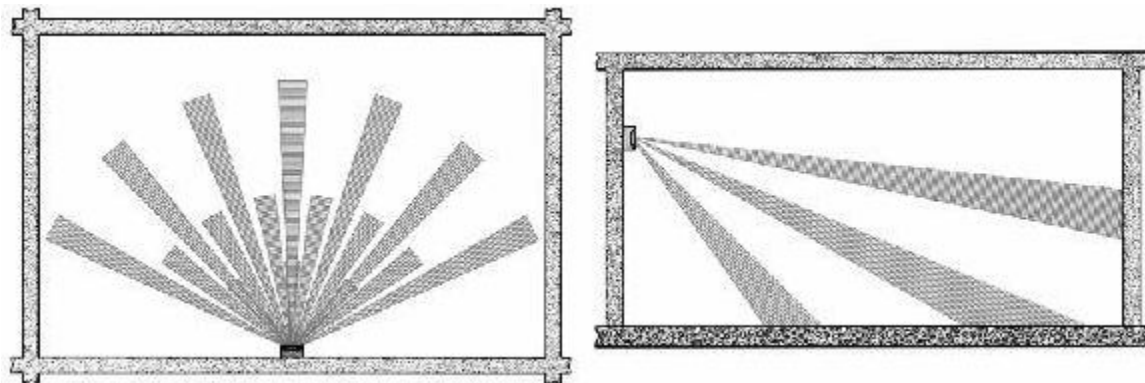


Figure LSS+4019 Active infrared motion sensor (Exterior)

### 40\_3.6.1 Guidelines for Installation of IR Devices



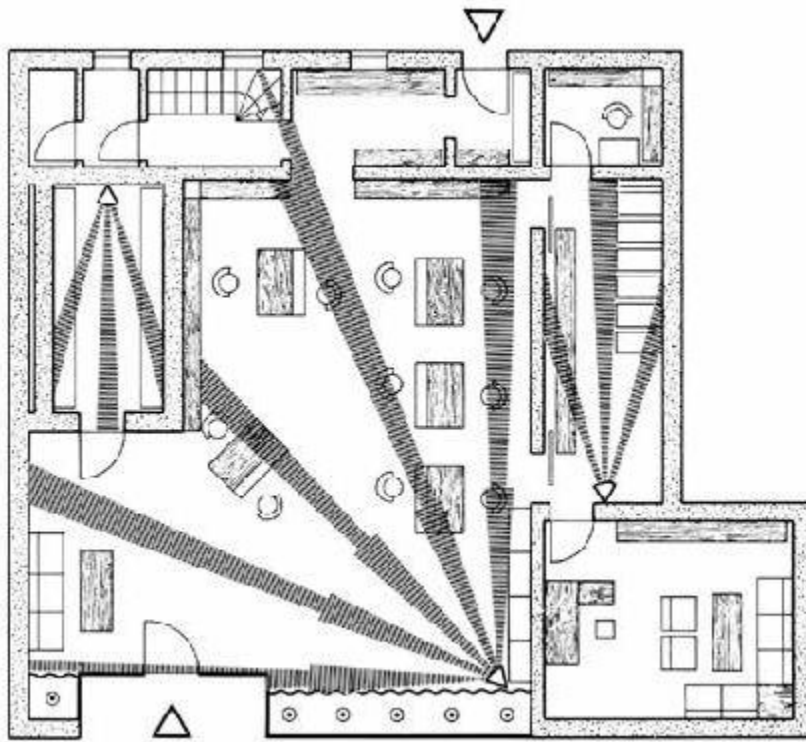
Although passive infrared detectors are an extremely reliable

component of an alarm system, they must be installed correctly to avoid loss of sensitivity and false alarms. The following guidelines apply:

- Sensors must not be installed so that they face the sun;
- Most sensors are designed for indoor use, although some "single beam" devices are available for external application;
- Use of different reflectors allows the coverage pattern to be modified. Thus, most sensors can be utilized for any surveillance requirement;
- A reduced monitoring angle allows for an increased range, and vice versa;
- Sensors can typically monitor an area of up to 60 meters, with a horizontal angle between 7°-120°;
- Depending upon the use (trap or room monitoring), the detector should be installed at a height of between 1.5-3 meters;
- Individual reflectors within a sensor can be manipulated to control coverage patterns;
- False alarms can be caused by detectors responding to rapid changes in radiated energy. Conditions that must be avoided will include:
  - Light bulbs being turned on and off;
  - A swinging lamp shade;
  - Filaments in fan connectors;
  - Sunlight interrupted by passing clouds;
  - Automobile headlights;
  - Humidity;
  - Sharp temperature changes;
  - Naked flames;
  - Direct sunlight.
- Pets can trigger an alarm. They should be kept out of areas that are monitored;
- Insects can cause a false alarm, thus an insect-repellent strip should be placed near the sensor;
- A detector can be desensitized by heating systems and warm-air vents. A sensor must be installed an adequate distance from heat sources;

- Ambient temperatures of 32 C to 38 C are unsuitable for fully effective operation of sensors;
- Furniture and other components can cause shadow zones in monitored areas because IR energy cannot penetrate such materials. These shadow zones provide the potential for compromise of the system and should be minimized;
- A sensor can be neutralized if its optical devices are covered with IR blocking materials before the alarm is set. Most sensors do not contain supervision circuitry to detect this condition;
- Sensors can be bypassed and compromised with insulating clothing having a low emissivity. This allows an intruder to appear to radiate the same temperature as the background. Many of the sensors will detect a change in the IR signature of a room, even if the temperature corresponds exactly with that of an intruder. In such a case, the radiation pattern and intensity of a moving person will change. If the sensor stores information about the "normal" signature, then the difference will be detected;
- Sensors can be activated by flash flames, or by hot water being poured under a door.





#### **40\_3.6.1.1 Defeat of Infrared and Other Heat Sensors**

There are many ways to defeat, bypass, or circumvent these devices. The techniques are summarized below, for exterior and interior applications.

##### **Heat Sensors**

- Avoidance, use of non-heat producing methods of attack;
- Bypass sensor circuits while the system is disarmed;

##### **Interior Sensors**

- Avoid the sensor. Use the walk-test light to determine boundaries of detection patterns while the system is disarmed;
- Mask the generation or detection of infrared energy by using petroleum jelly, Vaseline, silicone, hairspray, paint, or other foreign substance such as white-out, or an energy absorbing material such as cardboard;
- Utilize mylar covering that will not transmit any body heat;

- Block the detection of IR by taking advantage of man-made or natural barriers in the field of view of the sensor in order to allow penetration into the protection area;
- Use a cardboard box that is allowed to reach room temperature and is placed in the field of view of the sensor, thereby creating a corridor to run past the detection pattern;
- Introduce a higher temperature into the protected area, thus making the sensor less sensitive to temperature changes;
- Use very slow movement by the intruder as he advances toward the detector, taking advantage of the mounting location of the sensor;
- Bypass the sensor circuit while the system is disarmed;

### **Exterior Sensors**

- Avoidance of detection pattern;
- Tunneling under detection pattern;
- Bridging, two-man or pole vaulting over detection zone;
- Masking, by use of petroleum jelly, Vaseline, silicone, hairspray, paint or other foreign substance such as white-out or an energy absorption material such as cardboard;
- Blocking of the sensor, by taking advantage of natural or man made barriers in its field of view, to allow penetration past the detection area. Barriers such as washouts, depressions or snowfall will provide the required cover;
- Exploit detection sensitivity during high outside temperatures when the ambient temperature approaches skin temperature;
- Alarm stacking;
- Determine best intrusion path by walking directly into the sensor. This will reduce its detection capability.

## **40\_3.7 Video Monitoring Systems**



**LSS401: Video logging and capture systems**



**LSS403: DOE on alarm assessment**

Closed-circuit television can be effective for surveillance of a defined area. Local and remote monitoring of video images is now economically and technically feasible via the Internet. In the

photographs below, several wired (visible and covert) and wireless cameras are shown. Both monochrome and color cameras can be hidden virtually anywhere, and an image monitored at a remote location. Video can be stored on tape, hard drive, optical device, or solid state memory. Video surveillance systems are being employed to an ever increasing degree in public areas, transport, schools, and airports. Extremely sophisticated capture and logging systems have been implemented, especially at security check points, to allow for instant playback and transmission of images to law enforcement and security officers. See **chapter 39** for a more thorough discussion of video systems.

The inherent weakness of any video surveillance system is its operator, due to fatigue and monotony. Thus, an effective system must have the capability to direct the operator's attention to a specific camera display that is triggered by an alarm condition. An intruder must be easily recognized as a result of the image quality, field of view, and picture size. The system must be tamper-resistant, and alarm upon a loss of video. Recorders should operate in an automatic mode upon receipt of an alarm. All images must be buffered, so that there is no loss of data for pre-alarm, alarm, and post-alarm conditions.







#### 40\_3.7.1 Video Motion Detector

Images from video cameras, low light level devices, and those that function in the IR range are fed to motion detection sensors to provide for alarm notification in case of intrusion. The systems allow human evaluation of an alarm condition and also provide the means to document the event. These systems employ sophisticated processors to constantly compare a captured image and the "current" view, or compare images in sequence to detect changes in targeted areas. Any movement in the target field, or a

substantial change in lighting over a short period can trigger an alarm.

Video motion detection and analysis systems allow the manipulation of images in terms of zoom, pan, tilt, focus, and contrast, to permit the targeting of specified areas of a picture. Audio monitoring features may also be available. In some instances, cameras are secreted throughout a protected area; in other cases, they are visible and act as a deterrent.

Cameras must be properly installed, positioned, and set to protect the intended area and capture relevant images. Care should be taken to analyze lighting conditions to insure that the target area is sufficiently lit to insure the capture of a useable image.

The use of video as a monitoring system has many applications both overt and covert, and provides excellent redundancy to existing alarm sensors. Some examples of the use of video include:

- **Dead zones between two fences;**
- **Security check points;**
- **Gates;**
- **Fence lines;**
- **Outside storage lots;**
- **Interiors of warehouses (particularly at night);**
- **Approaches to "rear doors";**
- **Vehicle/pedestrian entry points;**
- **Loading docks;**
- **Guard posts where the CCTV system can be tied to a Duress Alarm;**
- **Secure internal areas, such as counting rooms, alarm centers, equipment storage, telephone and communications centers;**
- **Interview and interrogation rooms.**

Installation guidelines include:

- **Securely mount the cameras;**
- **Deny easy access to cameras and mounts, as well as video recorders that capture information;**
- **Maintain the field of view of the camera as open and uncluttered as possible;**



- **Reduce or eliminate vegetation and obstacles to visual observation.**

Unreliable or erratic operation will result under the following conditions:

- **Camera pointed towards high intensity lighting;**
- **Poor lighting characteristics or extended periods of darkness in targeted zone;**
- **Improper hardware selection. In some circumstances, low light level or IR sensitive cameras may be better suited to the task;**
- **Improper placement of the camera that does not allow a full field of view of the target area;**
- **Changes in angle of lighting from the sun;**
- **Changes in brightness from movement of cloud motion;**
- **Wind-blown objects passing in the target area;**
- **Camera vibration due to wind;**
- **Light source interference, such as from reflected light, headlights, traffic lights, or security lights pattern change;**
- **Flying insects near the lens;**
- **Dirty or dust-covered lens.**

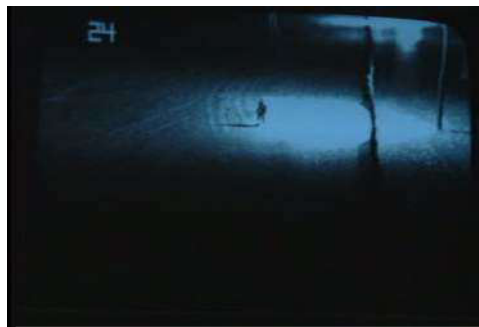
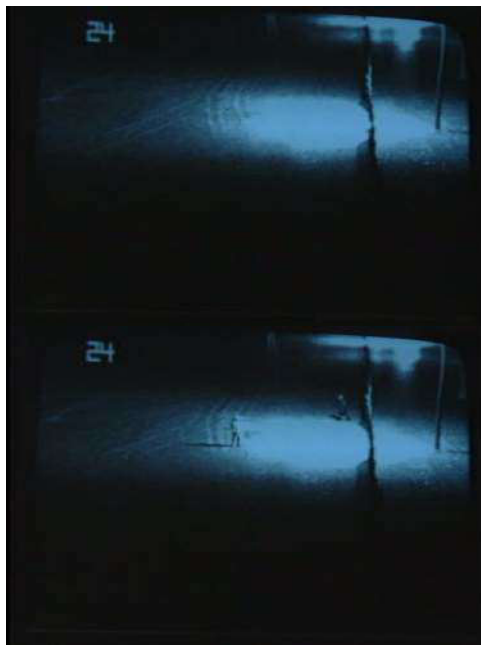
#### **40\_3.7.2 Defeat of Video Systems**

Improperly installed or maintained systems can be bypassed or neutralized through a variety of techniques that are described in this section. If a knowledgeable intruder can determine the coverage area of the camera, he may be able to avoid detection by moving around, under, or over the field of view. Camera systems can be defeated by blinding, stacking, camouflage or concealment from view. Defense-in-depth, providing for supplemental systems such as motion sensing, should always be deployed to provide for reliable detection. Primary security issues that involve video hardware include:

- **Video multiplexers can be disabled, which will result in a failure to monitor any camera;**
- **Blinding of the camera through the use of infrared light sources;**
- **Stacking of alarms to distract the operator;**
- **Camouflage or concealment of intruders;**
- **Programming errors, either deliberate or inadvertant, may**

render the system insecure;

- Monitors can be viewed by non-security personnel;
- Cameras can be destroyed or damaged. Lenses can be smashed or sprayed with material to make them unusable;
- Video recorders may not be properly maintained, resulting in dirty recording heads, erratic mechanical operation, or tape jams;
- Video recorder input settings may be tampered with;
- Tapes can be stolen;
- Failure to properly archive tapes;
- Storage of tapes near strong magnetic fields;
- Failure to maintain a retention policy;
- Use of poor quality or substandard tapes;
- Use of old time-lapse recording technology which is inherently unstable;
- Use of old tape with drop out errors or media failure;



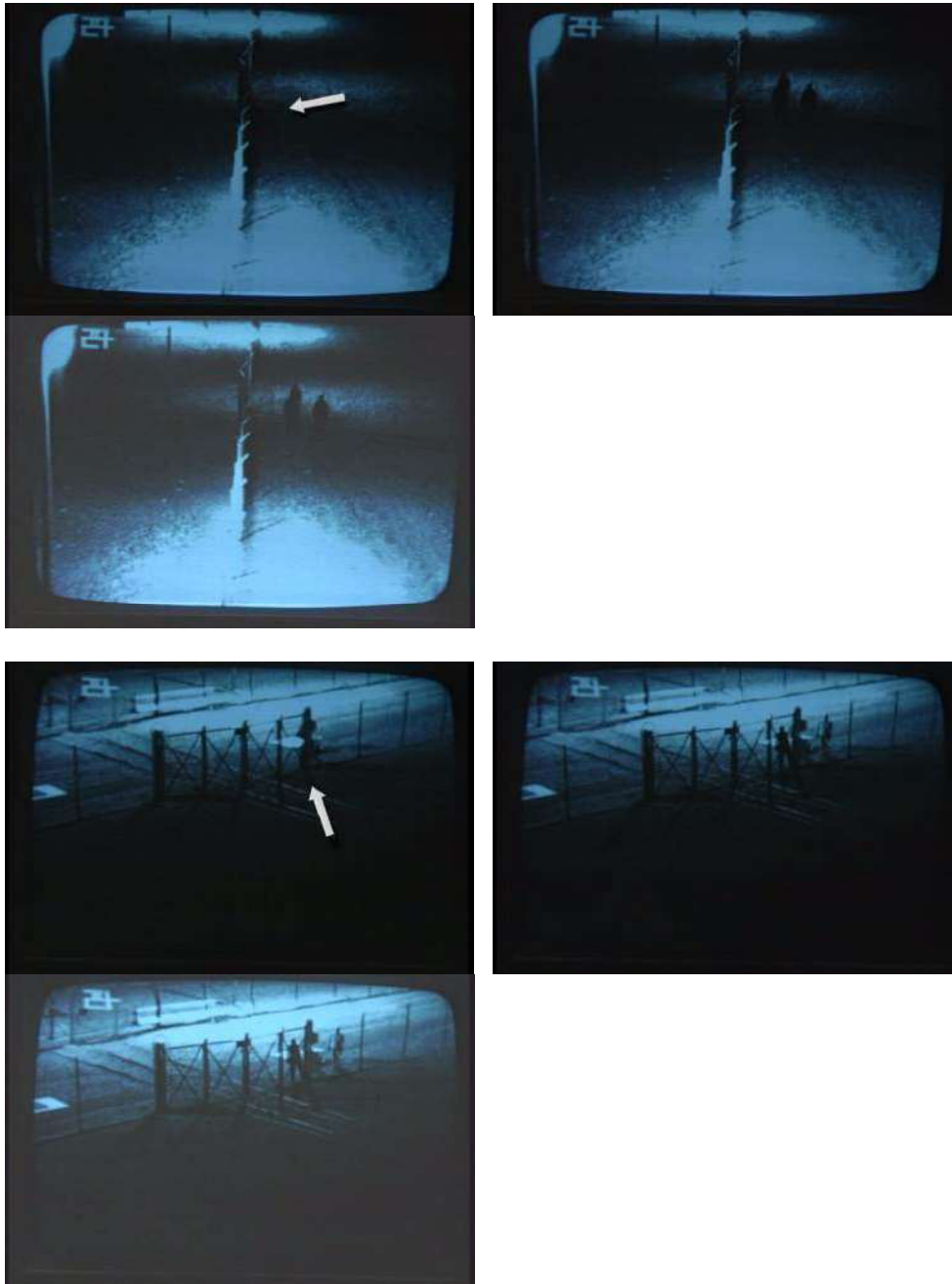
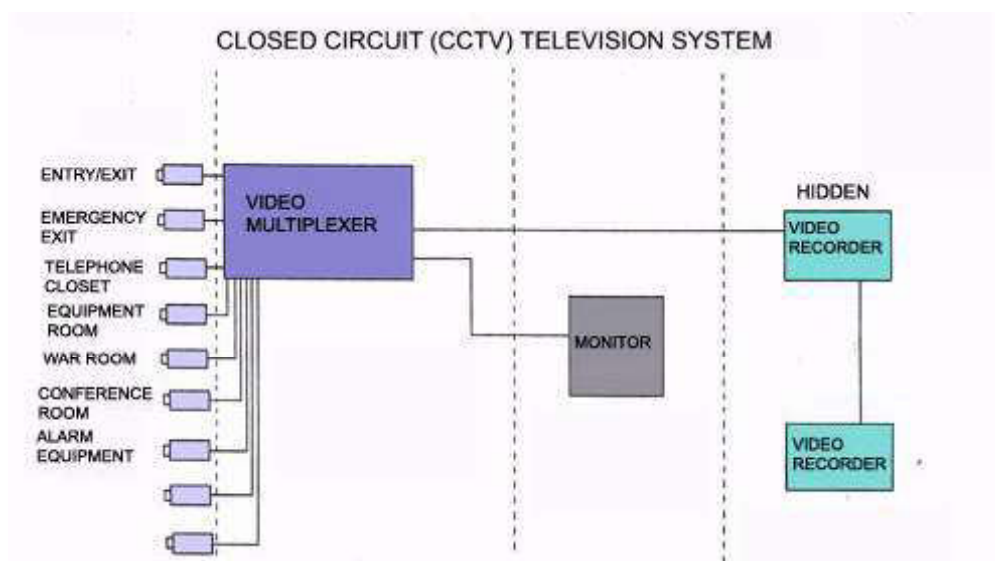


Figure LSS+4054 A camera is blinded by bright light in the photographs in the top and middle rows. Note the enhanced image (middle right) that shows the intruders. In the bottom row of photographs, the intruder is concealed, as shown in the enhancement (bottom right).

Courtesy of DOE Office of Security and Safety Performance Assurance.



#### 40\_3.7.2.1 Specific Defeat Techniques to Attack Camera Systems

There are a variety of means that can be employed to neutralize or destroy the effectiveness of a video surveillance system through attacks directed at cameras. These are summarized below. It is important for the security staff to analyze the potential methods to defeat the system, and to take corrective measures to minimize the risk. Reconnaissance by intruders will typically attempt to gather the following information:

- Learn the territory and any unique characteristics;
- Become familiar with every segment of the area of intrusion;
- Explore the area to be breached by day and night;
- Every alley, bush, tunnel, tree, building, wall, railing, fence or other accesible point will be explored, tested for alarms, and climbed;
- Typically, intruders will be careful not to traverse well-used paths, streets, alleys, or other areas that would normally be subject to surveillance;
- Intruders will look for areas of cover, especially if aerial surveillance is utilized;
- Consider that flares and smoke bombs may be utilized to blind surveillance equipment.

The following specific defeat techniques may be employed to reduce the reliability and effectiveness of any video

surveillance system, regardless of where the cameras are placed or mounted:

### **Plastic bag**

A plastic trash bag filled with glue can be utilized to take a camera out of service. Cameras are often "bagged" if they are to be repaired. Thus, such action may not draw undue attention.

### **Sticker and tape**

If the camera has been mounted so that it is accesible from the ground, then a sticker or tape can be placed over the lens to render it inoperative.

### **Paint gun**

A paint gun, water pistol, or aerosol spray can be utilized to damage the lens. This is a highly effective method that can be carried out within a few seconds. The action can disable many cameras within a short period of time. Spray glue also works well and will be more difficult to remove from the lens. Effective range can be 5 meters above the ground. Paint splatter may be left on perpetrators, so criminal investigators should check for such evidence.



### **Laser pointer or infrared light source**

A CCD or other video sensor can be disabled with a laser pointer or infrared light source. An emitter with an output of 5 milliwatts or greater can temporarily blind and may even permanently damage a video sensor. A threat from such devices has been recognized for their capability of damaging CCD and other pickup tubes, as well as the potential to cause eye damage or blindness to people up to several hundred feet from the

transmitter. Devices can be secreted in cameras with telephoto lenses or binoculars, and can be difficult or impossible to detect.

### **Cutting of coaxial cables**

Fiber optic, twisted pair, and coaxial cables can be severed or damaged with either a sharp hand axe, fence cutter, or garden pruning tools. When cables are cut, their repair or replacement may be time-consuming and costly. Pins, or the application of heat may also be utilized to break the transmission path, or short circuit the center conductor to ground, thereby preventing any signal from reaching a remote monitoring site.



### **Block drop**

Cameras can be damaged through the application of brute force by dropping weights, cinder blocks, or other objects from above their mounting location. Such action can completely destroy the housing and electronics.

### **High speed projectile**

A camera may be taken out of service if it is penetrated with a projectile such as a bullet from a rifle or handgun.

### **RF Interference for wireless transmitters**

Wireless cameras can be taken out of service by RF interference. Cameras will generally operate in the 900 MHz, 2.4 or 5.8 GHz bands, either on discrete frequencies, or utilizing spread spectrum. If the frequency band can be identified, the receiver can be jammed with a relatively high power signal, regardless of whether analog or digital transmission is employed. Spread spectrum and 802.11 protocol will not prevent this practice. Microwave ovens can also play havoc with 2.4 GHz receivers. This is a popular band for government covert operations, and is also utilized by the news media for remote pickups. Cameras operating with 802.11 protocol can also be received by computers equipped



with this technology. Most notebook computers incorporate WIFI. Inexpensive WIFI 802.11 sniffers are available to locate wireless networks.

## 40\_4.0 Protection for Specific Types of Premises, Construction, or Fixtures

A survey of alarm devices that can be used to protect specific structures or fixtures is provided as a reference.

### 40\_4.1 Windows

Windows and related components can be protected by the following devices:

- Alarm glass;
- Alarm glass with embedded wires;
- Bolt contacts;
- Glass-breakage detectors. They cannot be used on panes with shatter-resistant films, since the propagation characteristics of the medium is altered;
- Laminated glass with wire inserts;
- Security alarm glass;
- Light barriers;
- Magnetic contacts;
- Spanned wire;
- Surveillance foil;
- Transducers sensitive to changes in pressure;
- Vacuum alarm glass;
- Vibration contacts;
- Volumetric protection devices.

### 40\_4.2 Walls

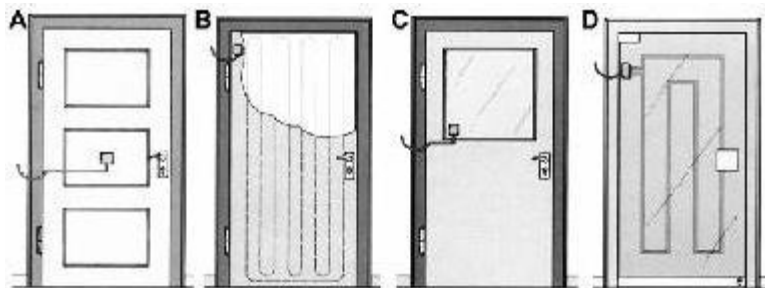
- Seismic detectors;
- Wallpaper coverings with embedded closed-circuit wiring.

#### 40\_4.2.1 Openings in Walls

- Taut-wire trips;
- Trap loops, consisting of cables or wires placed across openings at narrow intervals. Pressure or severance will trigger an alarm.

## 40\_4.3 Doors

- Magnetic contacts;
- Micro switch contacts;
- Bolt contacts;
- Light barriers;
- Vibration sensors;
- Surface surveillance systems (wires);
- Glass-breakage detectors;
- Sound detectors;
- Volumetric sensors;
- Foil.



Doors should always be protected by more than just magnetic switches; otherwise, they are subject to compromise. If burglars know the precise position of the trip, they can often cut around it and fix the magnet to the door frame.

## 40\_4.4 Small Openings and Confined Areas

- Dome lights: contacts to prevent the dome from being raised;
- Ventilation openings: tubing and wiring;
- Showcases: capacitance field change detectors or ultrasonic sensors;
- Drawers and doors of cabinets: magnetic contacts;

- **Locks and Locking Devices: bolt contacts;**
- **Furnishings: closed-circuit wiring in wallpaper.**

## **40\_4.5 Enclosed Rooms**

Entire rooms or specific areas or objects can be protected, depending upon exposure of property and character of the environment. The following devices can be utilized to protect enclosed rooms:

- **Volumetric sensors;**
- **Microwave detectors;**
- **Ultrasonic detectors;**
- **Passive infrared detectors;**
- **Proximity detectors.**

## **40\_4.6 Interior Surveillance**

Additional interior surveillance is usually necessary, regardless of the extent of protection and monitoring of the external shell. There are always exposed or vulnerable points of access that necessitate localized monitoring within the interior of a building. The following suggestions and guidelines are offered for the use and installation of internal trips:

- **Dead zones must be avoided in any scheme of protection;**
- **The operation of a detector must not be disturbed by external environmental influences;**
- **The risk of false alarms is high when traps are used for surveillance. They should only be installed in very controlled circumstances, as for instance in a small shop with few employees;**
- **Pressure mats can be placed under carpets and doormats;**
- **Large items or decorations can be monitored with magnetic contacts or micro switches;**
- **Contacts embedded within curtain rails will trigger whenever the curtains are closed;**
- **Current-sensing devices can be integrated into the electrical system to determine when interior**

lighting has been turned on or off or when power is drawn through the circuit;

- Ultrasonic approach switches can be utilized;
- Alarm panels must be installed in protected rooms;
- Silent alarms should be used in the event of holdup;
- Visible and audible alarms should be used for protection against burglary.

## 40\_4.7 Alarms in Banks

Physical devices and other safeguards must be implemented to insure that a burglary is detected at the earliest possible moment. Monitoring and protection of the perimeter and interior areas is essential. These include approaches to the bank, roofs, and windows. Within the interior spaces, it is imperative to provide localized surveillance of strong rooms, ATMs, and night depositories.

### 40\_4.7.1 Strong Rooms

Because of the prevalence of special forced entry materials and tools such as the thermic lance, diamond drills, and explosives, it is essential that strong rooms and safes be protected by many different physical barriers and alarm devices. These will include:

- Sound sensors for doors, walls, floors, and ceilings;
- Volumetric protection;
- Bolt or frame contacts for doors;
- Capacitance and motion detection systems for interior areas and safes;
- Smoke detectors to sense the use of a thermic lance;
- Charged conductors, sunk into or attached to walls;
- Closed-circuit television cameras and video recorders;
- Proximity sensors.

Interior safes and depositories may be further protected by an external casing that is alarmed. Automatic teller machines (ATMs) must also be specially monitored. Protection of the area around the ATM, as well as internal cash vaults, is essential.